Université du Québec en Outaouais

Département d'informatique et d'ingénierie

Thèse de doctorat :

Calcul du risque dans les systèmes de contrôle d'accès : approche basée sur le flux d'informations

Présenté dans le cadre des exigences du programme de

Doctorat en sciences et technologies de l'information

Sous la direction de :

Professeur Luigi Logrippo

Professeur Kamel Adi

Par

Sofiene Boulares

2017

Jury d’évaluation

Président du jury	Dr. Mohand Saïd Allili
Membre du jury	Dr. Guy-Vincent Jourdan
Membre du jury	Dr. Michel Iglewski
Membre du jury	Dr. Ana Cavalli
Directeur de recherche	Dr. Luigi Logrippo
Co-directeur de recherche	Dr. Kamel Adi

Remerciements

Je tiens d'abord à adresser mes plus sincères remerciements à mon directeur de thèse, Professeur Luigi Logrippo qui a encadré ce travail de manière avisée. L'intérêt qu'il a manifesté tout au long de ce projet de recherche, son soutien, sa disponibilité, sa patience, sa persévérance, sa rigueur ainsi que sa lecture méticuleuse de chacun des chapitres de cette thèse, ont sans aucun doute été la clé de l'aboutissemnt de ce travail.

Ma reconnaissance s'adresse également à mon co-directeur de thèse, Professeur Kamel Adi pour son appui scientifique, son engagement, sa disponibilité, la pertinence et la justesse de ses conseils, et lui adresse mes vœux de succès pour ses nouveaux projets.

Je remercie également les membres du jury Professeur Mohand Saïd Allili, Professeur Guy-Vincent Jourdan, Professeur Michel Iglewski et Professeur Ana Cavalli pour leurs suggestions enrichissantes.

Je tiens aussi à remercier le conseil de recherche en sciences naturelles et en génie du Canada (CRSNG) pour avoir subventionné ce travail.

Mes remerciements vont aussi aux membres de ma famille pour leur soutien inconditionnel et leurs encouragements.

Résumé

Les entreprises dépendent de l'information pour répondre à leurs besoins d'affaires. C'est pour cela que des systèmes de contrôle d'accès sont mis en place pour assurer la protection des informations contre la divulgation, l'altération et la destruction. Cependant, ces systèmes se basent généralement sur des décisions d'accès prédéterminées qui peuvent être trop rigides et ne pas permettre de répondre aux besoins évolutifs d'accès. D'où l'intérêt des systèmes qui étendent les concepts de contrôle d'accès traditionnels et permettent de prendre des décisions d'accès en évaluant le risque associé aux requêtes d'accès.

Dans cette thèse, nous proposons une approche dynamique basée sur le flux d'informations pour le calcul du risque des requêtes d'accès. Cette méthode peut être vue comme une approche de calcul du risque de la violation d'une politique de sécurité suite à un accès légitime. Notre approche considère plusieurs facteurs à savoir la fiabilité des sujets, la sensibilité des données, l'action demandée, l'historique des accès et les mesures de sécurité mises en place. Elle consiste essentiellement à suivre une procédure dont les étapes principales sont les suivantes :

1. calcul de la classification des objets et de l'habilitation des sujets en considérant les flux d'informations générés par les accès effectués dans le passé,
2. calcul de la potentialité de la menace de la requête d'accès en considérant les flux d'informations qui pourraient résulter si l'accès était permis ainsi que les mesures de sécurité mises en place,
3. calcul de l'impact en considérant les flux d'informations qui pourraient résulter si l'accès était permis ainsi que les mesures de sécurité mises en place,
4. calcul du risque de la requête d'accès, prenant en considération le résultat des calculs précédents.

Abstract

Organizations are dependent upon information to do business and information requires protection for confidentiality, integrity and availability. In most traditional access control systems, access decisions are predetermined and policies are rigid. However, in practice organizations need to use flexible methods where the decisions are determined dynamically. Risk-based access control extends traditional access control to provide support for flexible decision-making and to facilitate information sharing by determining the security risks associated with access requests, taking into consideration the evolution of the system.

In order to calculate risk values for access requests, we identify and formally describe a set of properties to be satisfied in an approach that is both formal and flexible, and which is motivated with a number of different examples, showing that it meets real-life organizational requirements.

Our risk calculation approach for access requests is based on the following steps:

1. calculation of the classifications of objects and clearances of subjects by considering the information flow generated by accesses which have been made in the past,
2. calculation of the threat likelihood of the access request by considering the information flow that could result if access is allowed and the security measures,
3. calculation of the impact of the access request by considering the information flow that could result if access has been allowed and the security measures, and
4. calculation of the risk of the access request, taking into consideration the results of the preceding calculations.

Publications

Les idées présentées dans cette thèse ont fait l'objet des publications suivantes :

1. Sofiene Boulares, Kamel Adi, Luigi Logrippo: Insider Threat Likelihood Assessment for Flexible Access Control. MCETECH 2017: 77-95
2. Sofiene Boulares, Kamel Adi, Luigi Logrippo: Insider Threat Likelihood Assessment for Access Control Systems: Quantitative Approach. FPS 2016: 135-142
3. Sofiene Boulares, Kamel Adi, Luigi Logrippo: Information Flow-Based Security Levels Assessment for Access Control Systems. MCETECH 2015: 105-121
4. Hemanth Khambhammettu, Sofiene Boulares, Kamel Adi, Luigi Logrippo: A framework for risk assessment in access control systems. Computers & Security 39: 86-103 (2013)
5. Hemanth Khambhammettu, Sofiene Boulares, Kamel Adi, Luigi Logrippo: A Framework for Threat Assessment in Access Control Systems. SEC 2012: 187-198
6. Sofiene Boulares, Kamel Adi, Luigi Logrippo: Information Flow-Based Security Levels Assessment for Access Control Systems. Article à soumettre à une revue.

Les textes intégraux des articles 1, 2, 3, 4 et 5 sont disponibles respectivement via les liens suivants :

https://link.springer.com/chapter/10.1007/978-3-319-59041-7_5

http://www.site.uottawa.ca/~luigi/papers/16_FPS.pdf

http://link.springer.com/chapter/10.1007%2F978-3-319-17957-5_7

http://www.sciencedirect.com/science/article/pii/S0167404813000552#

http://link.springer.com/chapter/10.1007%2F978-3-642-30436-1_16

Liste des abréviations, sigles et acronymes

Abréviation	Langue	Signification
ABAC	(Ang)	Attribute-Based Access Control
BLP	(Ang)	Bell–LaPadula Model
DAC	(Ang)	Discretionary Access Control
DoD	(Ang)	Department of Defense
HWM	(Ang)	High Water Mark
ISO	(Ang)	International Organization for Standardization
LWM	(Ang)	Low Water Mark
MAC	(Ang)	Mandatory Access Control
MLS	(Ang)	Multi-Level System
RBAC	(Ang)	Role-Based Access Control
UCON	(Ang)	Usage Control
XACML	(Ang)	eXtensible Access Control Markup Language
NIST	(Ang)	National Institute of Standards and Technology
ISACA	(Ang)	Information Systems Audit and Control Association
MEHARI	(Fr)	Méthode harmonisée d'analyse des risques
CLUSIF	(Fr)	Club de la Sécurité de l'Information Français
FIPS	(Ang)	Federal Information Processing Standards
OWASP	(Ang)	Open Web Application Security Project

Table des matières

Liste des figures

Liste des tableaux

Chapitre 1 : Introduction

1.1 Introduction générale

Les organisations dépendent de l'information pour mener leurs activités et conduire leurs affaires. Pour cette raison, la protection de l'information contre la divulgation, l'altération, la destruction et la fraude, représente un besoin primordial et une obligation légale dans certains cas.

Le *contrôle d'accès* joue un rôle important pour protéger les informations. Il consiste à vérifier si un *sujet* (normalement un processus, mais aussi une personne ou un dispositif) demandant l'exécution d'une *action* (lire, écrire, etc.) sur un *objet* (fichier, base de données, etc.), possède les droits nécessaires pour le faire [50]. Les décisions d'accès sont généralement prédéterminées hors ligne par l'administrateur de sécurité. Ces décisions statiques peuvent être trop rigides et ne pas permettre de répondre aux besoins réels et évolutifs d'accès. D'où l'intérêt des systèmes de contrôle d'accès, basés sur le *risque*, qui étendent les concepts de contrôle d'accès traditionnels pour faciliter le partage de l'information et répondre adéquatement aux besoins des entreprises.

Ces systèmes basés sur le risque permettent de prendre des décisions d'accès en tenant compte du risque associé aux requêtes. Ainsi, la permission ou l'interdiction d'une demande d'accès dépendra généralement du résultat de la comparaison de la valeur du risque calculée à la valeur du risque acceptable qui découle des besoins de sécurité de l'entreprise et qui représente sa tolérance au risque.

Toutefois, déterminer les décisions d'accès, est très souvent complexe et sujet à erreur. En effet, un système de contrôle d'accès qui attribue aux employés des accès non pertinents peut être à l'origine des incidents de sécurité internes. Selon la firme américaine de recherche et d'analyse *Forrester*, des incidents à l'intérieur des organisations sont à l'origine de *46 %* des brèches de sécurité, contre *33 %* pour les brèches de sécurité qui sont les résultats des attaques informatiques externes [87]. De plus, l'enquête *Global Corporate IT Security Risks 2013* [63], réalisée par *Kaspersky*

Lab (un éditeur antivirus), indique que *85 %* des entreprises à travers le monde ont connu au moins un incident de sécurité informatique d'origine interne.

Bishop et al. [10] distinguent deux catégories de *menaces internes* :

1. la violation de la politique de contrôle d'accès en utilisant un accès autorisé,
2. la violation de la politique de sécurité par l'obtention d'un accès non autorisé.

La première catégorie regroupe les cas où un employé utilise ses accès légitimes pour effectuer une action qui viole la politique de sécurité : divulguer des données sensibles àune tierce partie, bloquer l'accès à une ressource, fournir des renseignements à un employé qui n'a pas le droitde les connaître, refuser l'accès à un utilisateur légitime, etc.

La deuxième catégorie regroupe les cas où un employé exploite une vulnérabilité du système comme un *débordement de tampon* (*buffer overflow*) [44] pour obtenir un accès dont il ne dispose pas.

L'approche de calcul du risque des requêtes d'accès que nous présentons dans le cadre de notre travail traite la première catégorie des menaces internes. En effet, notre méthode peut être vue comme une approche de calcul du risque de la violation d'une politique de contrôle d'accès suite à l'autorisation d'une requête d'accès.

Le calcul du risque de l'autorisation d'une requête interdite par une politique de contrôle d'accès, pourrait être très utile dans le cas d'une entreprise qui a besoin de déroger à sa politique, afin de répondre à ses besoins d'affaires changeants. Prenons l'exemple d'une requête d'accès en *écriture* d'un sujet, qui a un niveau de fiabilité *élevée***,** à des informations qui ont un niveau de sensibilité *bas*. Dans un système de contrôle d'accès traditionnel qui interdit aux sujets d'écrire à des niveaux inférieurs, cet accès doit être refusé**.** Cependant, dans le cas d'un système basé sur le risque, le même accès peut ne pas être refusé. En effet, une requête d'accès sera autorisée si le risque qui lui est associé est inférieur au niveau du risque acceptable et elle sera refusée si le risque, qui lui est associé, est supérieur au niveau du risque acceptable.

Cela dit, la détermination du risque d'une requête d'accès est une tâche complexe, qui nécessite la considération de plusieurs facteurs, tels que la fiabilité des sujets, la

sensibilité des données, l'action demandée, l'historique des accès, l'emplacement physique ou l'emplacement logique à partir duquel l'accès est demandé, etc. Dans cette thèse, nous proposons une approche formelle qui tient compte de certains de ces facteurs.

Deux objectifs de sécurité seront considérés dans cette thèse :

1. la *confidentialité* qui est la propriété selon laquelle les informations ne sont pas rendues accessibles ou divulguées à des personnes, entités ou processus non autorisés [56],
2. l'*intégrité* qui est la propriété de protection de l'exactitude et de l'exhaustivité des informations [56].

1.2 Niveaux de sécurité

Les informations présentent des degrés différents de sensibilité et de criticité. Pour cela, les entreprises disposent généralement d'un *plan de classification des informations* pour déterminer le niveau de criticité des informations et leur garantir un niveau de protection approprié [58, 93]. Ces niveaux de classification sont déterminés à l'aide d'une *échelle d'impact* propre à chaque entreprise et qui pourrait refléter le principe suivant : Plus l'impact de la divulgation, de l'altération d'une information, etc., est important, plus la classification de l'information est élevée.

L'accès aux informations classées par un employé, peut requérir l'obtention d'une *habilitation de sécurité* (*Top Secret, Secret, etc*.) via une procédure formelle. En d'autres termes l'habilitation représente le niveau de fiabilité d'un employé. Ainsi, plus un demandeur d'accès est fiable plus il peut accéder à des informations ayant des niveaux de classification plus élevés.

Les modèles de contrôle d'accès multi-niveaux tels que *Bell-LaPadula* [8] et *BIBA* [9] nécessitent l'attribution de niveaux d'habilitation fixes aux sujets et des niveaux de classification fixes aux objets. Ainsi, les accès dépendent essentiellement du niveau d'habilitation du demandeur d'accès, du niveau de classification de l'information et de l'action demandée. Dans la suite de ce travail, nous désignons les habilitations et les classifications par *Niveaux de sécurité*. Les niveaux de sécurité peuvent désigner les

niveaux de confidentialité ou les *niveaux d'intégrité.* Selon [83] et [67], la confidentialité est liée à la divulgation de l'information, tandis que l'intégrité est liée à la modification des informations. Dans l'approche que nous présentons dans cette thèse, nous considérons que lorsque les sujets et les objets reçoivent des informations, leurs niveaux de confidentialité peuvent augmenter puisque l'importance de la confidentialité de leur contenu peut augmenter alors que leurs niveaux d'intégrité peuvent diminuer puisque le degré d'exactitude de leur contenu peut diminuer.

Nous considérons que le transfert des informations entre sujets et objets peut provoquer le changement des niveaux de sécurité. Ces transferts d'informations peuvent être le résultat d'opérations de lecture ou d'écriture ou d'inférences. Tous nos exemples se réfèreront à ces trois cas même si le transfert d'informations peut être faisable à travers des canaux cachés [68, 102].

1.3 Approche de calcul du risque

La publication *NIST Special Publication 800-30 Revision 1* [90] et le dossier technique *La gestion des risques-Concepts et méthodes (Révision 1 du 28 janvier 2009)* du *CLUSIF* [22], sont des guides de gestion des risques liés à la technologie de l'information. Ces guides stipulent que le risque est fonction de la potentialité d'une menace et de l'impact : *Risque = f(Potentialité de la Menace , Impact)* où *f* est une fonction croissante avec les valeurs de la *potentialité de la menace* et de l'*impact*.

Selon l'*OWASP* (*Open Web Application Security Project*) [79], le *risque R* est le produit de la *potentialité L* d'un incident de sécurité et *son impact I* ($R = L \times I$). Nous adaptons comme point de départ la formule de calcul du risque de l'*OWASP* afin de définir une fonction de calcul du risque pour les accès. Ainsi, la formule que nous utilisons dans notre travail est la suivante :

$$Risque = Potentialité\ de\ la\ menace \times Impact$$

La contribution principale de notre travail sera de proposer une approche dynamique basée sur le flux d'information, où l'intervention humaine est réduite à sa stricte nécessité pour le calcul du risque des requêtes d'accès. Comme nous pouvons le voir

dans la *Figure 1*, notre approche consiste à suivre une procédure dont les étapes principales sont les suivantes :

1. le calcul de niveaux de sécurité des sujets et des objets en considérant les flux d'informations générés par les accès qui ont été effectués dans le passé,
2. le calcul de la potentialité de la menace de la requête d'accès en considérant les flux d'informations qui pourraient résulter, si l'accès a été permis, et les mesures de sécurité réductrices de la potentialité de la menace,
3. le calcul de l'impact de la requête d'accès en considérant les flux d'informations qui pourraient résulter, si l'accès a été permis, et les mesures de sécurité réductrices de l'impact,
4. le calcul du risque de la requête d'accès en fonction des valeurs calculées ci-dessus.

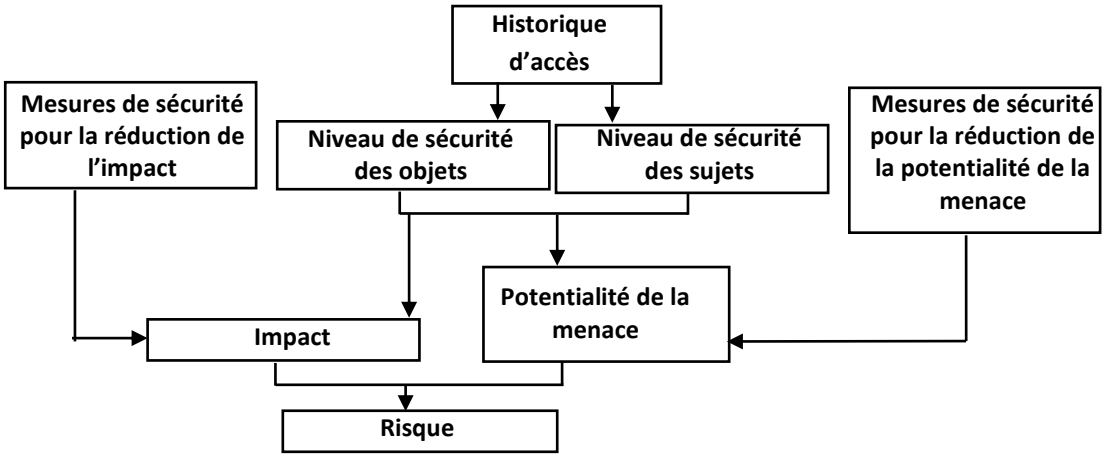


Figure 1. Approche pour le calcul du risque d'une requête d'accès

Le digramme de la *Figure 1* sera expliqué en détail dans cette thèse. Notons que les niveaux de sécurité des sujets et des objets sont utilisés tant que pour le calcul de la potentialité de la menace que pour le calcul de l'impact. Les mesures de sécurité sont des moyens de nature administrative ou technique qui permettent d'atténuer les risques.

Nous distinguons deux grandes familles de mesures de sécurité :

1. Les mesures de sécurité qui permettent de réduire la *potentialité de la menace*.

Exemple : la journalisation des accès, le chiffrement des données, etc.

2. Les mesures de sécurité qui permettent de réduire l'*impact*.

Exemple : les copies de sauvegarde.

Dans les chapitres *5*, *7* et *8*, nous présentons plus en détail les catégories des mesures de sécurité.

1.3.1 Calcul des niveaux de sécurité

Les *niveaux de sécurité* (habilitations et classifications), tels que les niveaux dans les *systèmes de contrôle d'accès multi-niveaux* (*MLS*) [65] devraient en théorie être exacts et corrects. En réalité, ces niveaux sont affectés de manière empirique et peuvent engendrer des politiques de sécurité trop restrictives ou trop permissives. Si ces niveaux étaient plus précis, ils pourraient être utilisés pour prendre de meilleures décisions de contrôle d'accès.

Dans ce travail, nous considérons que lorsque les sujets et les objets reçoivent les informations par des opérations de lecture dans le cas des sujets et des opérations d'écriture dans le cas des objets, les niveaux de confidentialité augmentent alors que les niveaux d'intégrité diminuent. Ces idées sont derrière les propriétés des modèles *MLS* mentionnés. Ainsi, nous proposons une approche qui permet de déterminer un *ordre de priorité* sur les niveaux de sécurité des sujets et des objets tout en tenant compte des inférences d'informations (association et agrégation d'informations) où des informations hautement classifiées peuvent être déduites à partir d'informations moins classifiées [31, 32, 33, 85]. Nous démontrons également que notre approche permet de calculer les *niveaux de sécurité*.

L'application de cette approche représente la première étape de notre méthode de calcul du risque des requêtes d'accès, qui se base principalement sur les *niveaux de sécurité*.

1.3.2 Hypothèses pour le calcul de la potentialité de la menace

Déterminer précisément la potentialité de divulgation ou d'altération des données, est une tâche complexe, car cela nécessite la prévision du comportement futur des utilisateurs.

Les modèles des menaces internes dans la littérature distinguent un ensemble de concepts en criminologie : la *capacité des utilisateurs*, la *motivation* et l'*opportunité* (modèle CMO) [86, 99-101].

La *capacité des utilisateurs* est d'un intérêt mineur pour le calcul de la *potentialité de la menace* dans le cas des dérogations aux politiques de contrôle d'accès parce que les risques sont censés provenir des activités d'un employé interne dans le cadre de son travail, plutôt que des attaques sophistiquées [7]. D'autre part, la *motivation* et l'*opportunité* sont d'une grande importance.

La première dimension de la *potentialité de la menace* est la *motivation*. Cette dimension est en lien avec les *caractéristiques personnelles* des utilisateurs qui permettent d'évaluer à quel point un groupe d'employés est fiable. Une étude réalisée par l'association des examinateurs certifiés de fraude (*Association of certified fraud examiners*) sur *1134* fraudes et incidents de sécurité, montre que la position hiérarchique des employés qui sont à l'origine des incidents de sécurité, affecte la fréquence des incidents [75]. En effet, selon *Cappelli et al.*, les employés internes à l'origine des menaces occupent généralement des positions en bas de la hiérarchie des entreprises [17]. Pour cela, nous faisons l'hypothèse que la motivation pour violer la politique de sécurité augmente lorsque le niveau de fiabilité des employés diminue. Dans notre approche, la *motivation* sera déterminée par le *niveau de sécurité du sujet*.

La deuxième dimension de la *potentialité d'une menace interne* est l'*opportunité* qui est causée par l'importance du privilège accordé lors d'une dérogation et le gain financier qui motive la plupart de ceux qui violent les politiques de sécurité [86]. L'*opportunité* représente la tentation causée par l'attribution du nouveau privilège en cas de dérogation. Cela plaide en faveur de l'idée présentée dans [4], « une opportunité fait un voleur ». Ainsi, nous pouvons supposer que l'*opportunité augmente* lorsque la

sensibilité de l'objet à accéder *augmente*. Dans notre approche, l'*opportunité* sera déterminée par le *niveau de sécurité de l'objet*.

D'après ce qui précède, nous supposons que la *potentialité de la menace* dépend de la distance entre le *niveau de sécurité* du *sujet* demandeur d'accès et le *niveau de sécurité* de l'*objet* demandé. Autrement dit, nous pouvons supposer une corrélation entre le *flux d'informations* qui peut résulter d'un accès permis et la *potentialité de la menace* d'une requête. En effet, un accès en *lecture* crée des flux d'informations de l'objet vers le sujet et un accès en *écriture* crée des flux d'informations du sujet vers l'objet. Certains *flux d'informations* sont plus importants que d'autres, en raison de leurs conséquences possibles. Par exemple, le flux d'informations d'un sujet ayant une habilitation *Top secret* vers un objet *Non classé* est plus dangereux sur la confidentialité des informations qu'un flux d'information crée par l'accès en écriture du même sujet à un objet qui a la classification *Secret*. Dans le premier cas, l'information *Top secret* pourrait être divulguée au public alors que dans le second cas, cette information resterait secrète. Pour cela, nous considérons que la *potentialité de la menace augmente* quand l'importance d'un flux d'informations qui pourrait résulter de la permission d'accès *augmente*.

Plus précisément, nous considérons que la *potentialité de la menace sur la confidentialité* augmente lorsque l'information passe à des niveaux de confidentialité moins élevés, et elle diminue lorsque l'information passe à des niveaux de confidentialité plus élevés. Cela s'explique par le fait que le passage de l'information vers le bas augmente la possibilité de sa lecture par des sujets non fiables. De même, la *potentialité de la menace sur l'intégrité* augmente lorsque l'information passe à des niveaux d'intégrité plus élevés, et elle diminue lorsque l'information passe à des niveaux d'intégrité moins élevés. Cela s'explique par le fait que le passage de l'information vers le haut augmente la possibilité de la dégradation de l'intégrité des informations aux niveaux d'intégrité élevés à cause des informations ayant un niveau d'intégrité bas.

En plus de la considération des flux d'informations, les mesures de sécurité qui permettent de réduire la *potentialité de la menace* seront également considerées dans notre approche.

Dans cette thèse, nous proposons une approche basée sur les flux d'informations qui permet de donner une estimation qualitative et quantitative des *potentialités de menaces*. Cette approche considère les facteurs suivants :

- l'objectif de sécurité visé (confidentialité ou intégrité),
- l'action demandée (lecture ou écriture),
- le niveau de confidentialité ou le niveau d'intégrité du sujet demandeur d'accès,
- le niveau de confidentialité ou le niveau d'intégrité de l'objet à accéder,
- les mesures de sécurité réductrices de la potentialité de la menace.

1.3.3 Hypothèses pour le calcul de l'impact

L'*impact* est une estimation des conséquences de la concrétisation du risque. Dans notre approche, sa valeur dépend du niveau de sécurité de l'objet, du sujet, de l'action demandée (sens du flux de l'information) et de l'objectif de sécurité visé.

L'intuition derrière cette approche de calcul de l'*impact* est que dans le cas des accès de lecture vers le haut où l'objectif de confidentialité est visé et des accès de lecture vers le bas où l'objectif d'intégrité est visé, les informations sont transférées des objets vers les sujets. Ainsi, nous considérons que la valeur de l'*impact intrinsèque* (l'impact sans considérer les mesures de sécurité mises en place) dépend des niveaux de sécurité des *objets*.

Dans le cas des accès d'écriture vers bas où l'objectif de confidentialité est visé et des accès d'écriture vers le haut où l'objectif d'intégrité est visé, les informations sont transférées des sujets vers les objets. Ainsi, nous considérons que la valeur de l'*impact intrinsèque* dépend des niveaux de sécurité des *sujets*. En effet, l'*impact intrinsèque* dépend du niveau de sécurité de l'entité (sujet ou objet) source de l'information. L'*impact intrinsèque* est *proprtionnel* au niveau de l'entité source de l'information dans le cas de la confidentialité. Il est *inversement proprtionnel* au niveau de l'entité source de l'information dans le cas de l'intégrité.

Par exemple, lorsque la confidentialité est visée, l'accès en lecture à un objet qui a un niveau de confidentialité *Secret* peut avoir un *impact intrinsèque* plus grand que l'accès

en lecture à un objet qui a un niveau de confidentialité *Non classé*. De même, l'accès en écriture d'un sujet qui a un niveau de confidentialité *Top Secret* peut avoir un *impact intrinsèque* plus grand que l'accès en écriture d'un sujet qui a un niveau de confidentialité *Secret*.

Des mesures de sécurité qui permettent de réduire l'impact intrinsèque sont considérées dans notre approche. Cette approche considère les facteurs suivants :

- l'objectif de sécurité visé (confidentialité ou intégrité),
- l'action demandée (lecture ou écriture),
- le niveau de confidentialité ou le niveau d'intégrité du sujet demandeur d'accès,
- le niveau de confidentialité ou le niveau d'intégrité de l'objet à accéder,
- les mesures de sécurité réductrices de l'impact.

1.3.4 Motivation

Considérons un système de contrôle d'accès qui gère l'accès à un nombre de dossiers. Les dossiers sont enregistrés dans une base de données et peuvent être accessibles par le biais d'un terminal distant. Dans le cas où il y a un besoin urgent de consulter le dossier d'un patient qui est classé *Top secret*, et que tous les membres du personnel durant leur service n'ont pas l'habilitation de lire son contenu, lequel des membres du personnel devrait être autorisé à lire le contenu de ce dossier et sur quelle base ?

La décision pourrait être basée sur une estimation des risques afin de nommer l'employé dont l'accès serait le moins risqué. L'approche que nous proposons dans le cadre de cette thèse permettra de répondre également aux questions suivantes : est-ce qu'un employé autorisé à accéder à ce dossier à un instant donné serait automatiquement autorisé à accéder à ce même dossier à un instant ultérieur ? Si un employé a été autorisé à lire le contenu de ce dossier, serait-il autorisé à le modifier? Est-ce que ce risque d'accèder au dossier est le même à partir de tous les terminaux ?

Notre approche permettra de répondre à ces questions, comme nous allons le voir dans le chapitre *9*, sur la base des idées suivantes : les décisions d'accès ne seraient pas nécessairement les mêmes à tous les instants puisque les niveaux de sécurité utilisés pour

la détermination de la valeur du risque seraient mis à jour en fonction de l'historique des accès. De plus, un accès autorisé en lecture ne serait pas automatiquement autorisé en écriture puisque le flux d'information dans le cas de la lecture est l'inverse de celui de l'écriture. Nous allons voir également que la valeur du risque calculée pourrait dépendre des *mesures de sécurité* mises en place à un emplacement et à un instant donné. Ces mesures de sécurité peuvent être de nature administrative ou technique (politique de sécurité, chiffrement des données, journalisation, etc.).

1.4 Contributions visées

Les contributions que nous visons dans ce travail sont les suivantes :

1. la présentation d'une approche pour calculer les *niveaux de sécurité* des sujets et des objets dans le chapitre *6*,
2. la présentation d'une approche pour calculer la *potentialité de menace* d'une requêted'accès dans le chapitre *7*,
3. la présentation d'une approche pour le calcul de *l'impact* d'une requête d'accès dans le chapitre *8*,
4. la présentation d'une approche générale pour le calcul du *risque* d'une requête d'accès dans les chapitres *5* et *9*.

Dans cette thèse, nous présentons la définition des principes de calcul des *niveaux de sécurité* des sujets et des objets, de la potentialité de la menace et de l'impact. Ces principes nous permettront de définir un ordre de priorité sur les *niveaux de sécurité,* sur les *potentialités de la menace* et sur l'*impact*. Des *formules* qui captent ces propriétés seront également présentées.

Les idées présentées dans cette thèse ont fait l'objet de nos articles [12, 13, 14, 60, 61].

1.5 Organisation de la thèse

Dans le chapitre *1*, nous avons présenté une description brève de notre approche de calcul du risque des demandes d'accès, la motivation de notre travail et les contributions visées. La suite de cette thèse est organisée comme suit :

Chapitre 2

Dans le chapitre *2*, nous nous référons à un ensemble de normes et méthodologies, en lien avec les domaines de la sécurité de l'information, le contrôle d'accès et la gestion du risque, pour présenter les concepts qui seront utilisés tout au long de la thèse.

Chapitre 3

Le chapitre *3* présente des modèles formels de contrôle d'accès en l'occurrence le contrôle d'accès basé sur des treillis (*LBAC*) [27], le modèle *Bell-LaPadula* [8], le modèle *Biba* [9], le modèle de la *muraille de Chine (Brewer et Nash)* [15], le *contrôle d'accès basé sur les rôles (RBAC)* [34, 35, 84], le *contrôle d'accès basé sur les attributs (ABAC)* [51] et le modèle du *contrôle de l'usage* (*UCON)* [80].

Chapitre 4

Le chapitre *4* présente un ensemble de travaux sur les systèmes de contrôle d'accès basé sur le risque notamment des méthodes d'estimation quantitative ou qualitative du risque. Certains de ces travaux présentent des cadres généraux pour la gestion du risque dans les systèmes de contrôle d'accès.

Chapitre 5

Dans le chapitre *5*, nous présentons les étapes de notre approche de calcul du risque des requêtes d'accès et nous définissons une fonction d'estimation du risque pour les accès.

Chapitre 6

Dans le chapitre *6*, nous présentons notre approche pour le calcul des niveaux de sécurité des sujets et des objets en considérant les flux d'informations résultants des accès passés. Cette évaluation représente la première étape pour le calcul du risque d'une requête d'accès selon notre approche.

Chapitre 7

Dans le chapitre *7*, nous décrivons notre approche pour le calcul de la *potentialité de la menace*, une étape essentielle pour le calcul du risque selon l'approche que nous proposons.

Chapitre 8

Dans le chapitre *8*, nous décrivons notre approche pour le calcul de l'impact, une étape essentielle pour le calcul du risque selon l'approche que nous proposons.

Chapitre 9

Dans le chapitre *9*, nous présentons l'application de notre approche au modèle de contrôle d'accès basé sur les attributs *ABAC*, nous comparons notre approche à un ensemble d'approches pour montrer sa pertinence, nous montrons l'intérêt de l'utilisation de notre approche, et nous présentons un cas d'application.

Chapitre 10

Le chapitre *10* présente l'outil que nous avons implémenté pour démontrer l'applicabilité de notre approche.

Chapitre 11

Nous concluons cette thèse par la presentation d'un sommaire des contributions de notre travail de recherche. Nous présentons aussi les avantages de notre approche par rapport aux travaux connexes, et les orientations futures possibles de notre recherche.

Chapitre 2 : Concepts généraux

2.1 Introduction

Dans le cadre de ce travail, nous abordons trois domaines à savoir *la sécurité de l'information*, le *contrôle d'accès* et la *gestion du risque*. Dans ce chapitre, nous nous référons à un ensemble de normes et méthodologies, qui font autorité dans ces domaines, pour présenter les concepts qui seront utilisés tout au long de ce document. Dans la suite, nous donnerons des définitions plus précises à plusieurs de ces concepts, normalement sans trahir leur signification usuelle.

2.2 Sécurité de l'information

La *sécurité de l'information* est un terme qui se réfère à la confidentialité, l'intégrité et la disponibilité de l'information [56].

Confidentialité

La *confidentialité* est la propriété selon laquelle l'information n'est pas rendue accessible ou divulguée à des personnes, entités ou processus non autorisés [56].

Intégrité

L'*intégrité* est la propriété de protection de l'exactitude et de l'exhaustivité des informations [56].

Disponibilité

La *disponibilité* est la propriété d'une information d'être accessible et utilisable à la demande par une entité autorisée [56].

Renseignements personnels

Les *renseignements personnels* sont les renseignements, quels que soient leur forme et leur support, concernant un individu identifiable, notamment les renseignements relatifs à sa race, à son origine nationale ou ethnique, à sa couleur, à sa religion, à son âge, à sa

situation de famille, à son dossier médical, à son casier judiciaire, à ses antécédents professionnels, à des opérations financières auxquelles il a participé, etc. [70].

Incident lié à la sécurité de l'information

Un *incident lié à la sécurité de l'information* est un événement intéressant la sécurité de l'information, indésirable ou inattendu, et présentant une probabilité non-négligeable de compromettre les opérations liées à l'activité de l'organisme et de menacer la sécurité de l'information [21].

2.3 Contrôle d'accès

Le *contrôle d'accès* consiste à déterminer les activités autorisées aux utilisateurs légitimes lorsque ces derniers demandent d'accéder à des ressources. Le contrôle d'accès est utilisé par les systèmes d'exploitation pour protéger les fichiers et les répertoires, ainsi que par les systèmes de gestion de base de données pour protéger les tables et les vues, etc. [50].

Objet

Un *objet* est une entité qui contient des informations. L'accès à un objet implique potentiellement l'accès à l'information qu'il contient [76].

Sujet

Un *sujet* est une entité active (normalement un processus, mais aussi une personne ou un dispositif) qui provoque le transfert de l'information d'un objet à un autre [76].

Opération

Une *opération* est une action sur un fichier invoqué par un sujet. Par exemple, lecture, écriture, suppression, etc. [35].

Permission

Une *permission* est une autorisation d'effectuer une opération sur un objet. Par exemple, un caissier de banque peut disposer des autorisations, ou permissions, pour exécuter des opérations de débit et de crédit sur les dossiers des clients [35].

Séparation des pouvoirs

La *séparation des pouvoirs* est le principe qui stipule qu'aucun utilisateur ne peut avoir un ensemble de privilèges qui lui permettent d'abuser du système. Par exemple, la personne qui autorise un salaire ne doit pas être aussi celle qui peut le payer. Dans un système de sécurité basé sur les rôles, la séparation des pouvoirs peut être appliquée de façon statique en définissant les rôles qui ne peuvent être assignés à un même utilisateur ou de façon dynamique en appliquant un contrôle des permissions au moment de l'accès [50].

Besoin d'en connaitre (Need to know)

Le principe du *besoin d'en connaitre* ou *besoin de savoir* stipule qu'un processus ne devrait avoir accès qu'aux objets dont il a besoin pour accomplir sa tâche, et dans les modes pour lesquels il a besoin d'accès et uniquement pendant des laps de temps déterminés [24].

Moindre privilège (Least privilege)

Le principe du *moindre privilège* stipule que chaque utilisateur doit avoir seulement les autorisations nécessaires pour accomplir ses tâches dans son organisation. L'usager doit avoir le moindre privilège possible pour qu'il ne puisse pas abuser des permissions dont il n'a pas besoin [43].

Finalité

La *finalité* est la raison de la collecte et de l'utilisation des données [16].Une information peut être disponible, mais seulement pour certaines finalités. Par exemple, les renseignements personnels d'un patient doivent être communiqués seulement aux membres de l'équipe de soins de santé qui ont besoin de les connaître et seulement pour lui fournir les soins nécessaires.

Classification

Un niveau de *classification* indique l'importance des informations et détermine les exigences de sécurité spécifiques applicables à ces informations. Des niveaux de

classification (*Top Secret, Secret, etc*.) clairement définis sont essentiels à un système de classification efficace [48].

Habilitation

Une *habilitation* de sécurité est un statut attribué à un employé (*Top Secret, Secret, etc*.), qui pourrait lui permettre d'accéder à des informations classées. Une *habilitation* de sécurité à elle seule n'accorde pas à son détenteur l'accès aux informations classées. Afin d'avoir accès aux informations, un employé doit également avoir un *besoin d'en connaître* [93]. L'habilitation d'un sujet détermine souvent ses permissions.

Politique de contrôle d'accès

Une *politique de contrôle d'accès* est un ensemble de règles de haut niveau selon lesquelles le contrôle d'accès doit être déterminé [82].

Modèle de contrôle d'accès

Un *modèle de contrôle d'accès* fournit une représentation formelle d'un mécanisme pour appliquer des politiques de contrôle d'accès. La formalisation permet de prouver que le système de contrôle d'accès qui implémente le mécanisme applique correctement les politiques de contrôle d'accès considérées [82].

2.4 Risque

Le concept de risque a une portée très vaste. Nous trouvons donc plusieurs définitions de ce concept. Dans ce qui suit, nous présentons quelques-unes que nous avons jugées pertinentes pour la compréhension de notre travail.

Le *risque* est la combinaison de la probabilité d'un évènement et de sa conséquence [57].

Le *risque* est l'effet de l'incertitude sur l'atteinte des objectifs [53].

Le *risque informatique* est la possibilité qu'une menace donnée puisse exploiter des vulnérabilités et causer des dommages à l'organisation [57].

Le *risque intrinsèque* est une estimation maximaliste du risque, en dehors de toute mesure de sécurité [23].

Exemple : divulgation des renseignements personnels, indisponibilité des services et altération des données.

Menace

Une *menace* est la cause potentielle d'un incident indésirable, pouvant entraîner des dommages au sein d'un système ou d'un organisme [56].
Exemple : modification de données après intrusion.

Vulnérabilité

Une *vulnérabilité* est une faiblesse d'un bien ou d'un groupe de biens pouvant faire l'objet d'une menace [54].
Exemple : pare-feu mal configuré.

Potentialité

La *potentialité* du risque représente, en quelque sorte, sa probabilité d'occurrence, bien que cette occurrence puisse ne pas être modélisable en termes de probabilité [23].

La *potentialité intrinsèque* du risque est une estimation maximaliste de sa probabilité d'occurrence, en dehors de toute mesure de sécurité.

Impact

L'*impact* du risque sur l'entreprise représente la gravité des conséquences directes et indirectes qui découleraient de l'occurrence du risque [23]. L'occurrence du risque étant la divulgation ou l'altération ou la non-disponibilité de données.
Exemple : dégradation de la réputation d'une entreprise.

L'*impact intrinsèque* est une estimation maximaliste des conséquences du risque, en dehors de toute mesure de sécurité [23].

Estimation qualitative

L'*estimation qualitative* utilise une échelle d'attributs qualificatifs pour décrire l'ampleur des conséquences potentielles d'un événement ainsi que la probabilité de son occurrence [56] (par exemple : faible, moyenne et élevée).

Estimation quantitative

L*'estimation quantitative* utilise une échelle comportant des valeurs numériques (plutôt que les échelles descriptives utilisées lors de l'estimation qualitative), à la fois pour les conséquences et pour la potentialité, à l'aide de données obtenues à partir de sources diverses. La qualité de l'analyse dépend de la précision et de l'exhaustivité des valeurs numériques et de la validité des modèles utilisés [57].

Mesures de sécurité

Une *mesure de sécurité* est un moyen de gérer un risque, comprenant des politiques, des procédures, des lignes directrices, et des pratiques ou structures organisationnelles, et pouvant être de nature administrative, technique, ou juridique. Dans [57], les termes *contrôle* et *contre-mesure* sont également utilisés comme synonymes de *mesure de sécurité*.

Dans ce qui suit, nous distinguons six types de mesures de sécurité :

- Les *mesures structurelles* qui diminuent l'exposition naturelle au risque. En effet, devant une situation de risque donnée qui pourrait être causée par l'autorisation d'un accès, les organisations ne sont pas égales [23].
  Exemple : une organisation qui traite et sauvegarde des renseignements personnels (hôpital, organisme gouvernemental, etc.) serait plus exposée au risque de divulgation des données, qu'une autre organisation qui ne sauvegarde que des données publiques.
- Les *mesures dissuasives* ou de prévention avancée qui permettent de décourager les agresseurs humains d'exécuter une menace potentielle. Pour être efficaces, ces mesures doivent reposer sur une bonne connaissance des techniques et capacités des agresseurs humains redoutés [23].
  Exemple : la journalisation des accès.
- Les *mesures préventives* qui empêchent une menace d'atteindre des ressources du système d'information [23].
  Exemple : le chiffrement des données.

- Les *mesures protectives* qui visent à limiter l'ampleur des détériorations éventuelles conséquences de l'exécution d'une menace [23].
  Exemple : les alertes suite à la détection d'une intrusion logique.
- Les *mesures palliatives* qui sont destinées à minimiser les conséquences, au niveau de l'activité ou de l'entreprise, des détériorations dues à un sinistre [23].
  Exemple : les copies de sauvegarde.
- Les *mesures récupératives* qui visent à réduire le préjudice subi par transfert des pertes sur des tiers, ou par attribution de dommages et intérêts consécutifs à des actions de justice [23].
  Exemple : les assurances.

Analyse du risque

L'*analyse du risque* est l'utilisation systématique d'informations pour identifier ses sources et l'estimer [57].

Évaluation du risque

L'*évaluation du risque* est le processus de comparaison du risque estimé avec des critères de risque donnés pour en déterminer l'importance [57].

Appréciation du risque

L'*appréciation du risque* est l'ensemble des processus d'analyse du risque et d'évaluation du risque [57].

Gestion du risque

La *gestion du risque* est l'ensemble des activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque [57].

Traitement du risque

Le *traitement du risque* est le processus de sélection et de mise en œuvre des mesures visant à diminuer le risque [57].

Acceptation du risque

L'*acceptation du risque* est la décision d'accepter un risque [57].

Risque résiduel

Le *risque résiduel* est le risque subsistant après le traitement du risque [57].

2.5 Conclusion

La liste des définitions présentées dans ce chapitre n'est pas exhaustive, d'autres définitions en lien avec les domaines de la *sécurité de l'information*, du *contrôle d'accès* et de la *gestion du risque* existent. Cependant, nous avons choisi les définitions qui permettront de faciliter la compréhension des idées qui seront présentées dans les chapitres suivants.

Chapitre 3. État de l'art 1 : Modèles formels de contrôle d'accès

3.1 Introduction

Le *contrôle d'accès* est une composante importante de la sécurité des systèmes d'information. Il consiste à vérifier si un sujet (un utilisateur humain, un processus, etc.) demandant l'accès (lecture, écriture, modification, etc.) à un objet (un fichier, une base de données, etc.) a les droits nécessaires pour le faire.

L'application de la politique de contrôle d'accès d'une organisation permet d'assurer des objectifs de sécurité (la disponibilité, l'intégrité et la confidentialité) qui peuvent être spécifiés de façon claire et non ambiguë par des modèles de contrôle d'accès.

La littérature identifie ces quatre familles principales de modèles de contrôle d'accès :

- les *modèles de contrôle d'accès discrétionnaires*,
- les *modèles de contrôle d'accès obligatoires*,
- les *modèles de contrôle d'accès basés sur les rôles*,
- les *modèles de contrôle d'accès basés sur attributs.*

Les *modèles de contrôle d'accès discrétionnaires* ou « *Discretionary Access Control* » (*DAC*) [65] tels que le modèle de *Lampson* [64] et le modèle de *Harrison Ruzzo Ullmann* [47] permettent à un sujet d'attribuer des droits d'accès à d'autres sujets. Ces modèles sont flexibles mais ils peuvent conduire à des erreurs non voulues par les sujets. Le contrôle d'accès discrétionnaire est généralement défini par opposition au contrôle d'accès obligatoire (*MAC*) [65].

Les *modèles de contrôle d'accès obligatoires* « *Mandatory Access Control* » ne permettent pas aux sujets d'intervenir dans l'attribution des droits d'accès et imposent des règles incontournables garantissant l'atteinte des objectifs de sécurité. Ces modèles sont plus rigides que les modèles de contrôle d'accès discrétionnaire mais plus sécures.

Le *contrôle d'accès basé sur les rôles* [34, 35, 84] « *Role Based Access Control* » (*RBAC*) est une approche alternative au *contrôle d'accès obligatoire* (MAC) et au *contrôle d'accès discrétionnaire* (*DAC*).

Le *contrôle d'accès basé sur les attributs* « *Attribute based access control* » (*ABAC*) [51] permet de déterminer les décisions d'accès en considérant les attributs des sujets, des objets, des actions et des conditions de l'environnement.

Dans ce chapitre, nous présentons des modèles formels de contrôle d'accès obligatoires qui sont généralement des modèles de *contrôle de flux* en l'occurrence le *contrôle d'accès basé sur les treillis* [27], le modèle *Bell-LaPadula* [8], le modèle *Biba* [9], le modèle de la *muraille de Chine* [15]. De plus, nous présentons le *contrôle d'accès basé sur les rôles RBAC* [34, 35, 84], le *contrôle d'accès basé sur les attributs ABAC* [51] et le modèle *contrôle de l'usage UCON* [80].

3.2 Modèles de contrôle de flux

Dans un système d'informations d'une organisation, l'accès aux objets donne lieu au passage de l'information d'un objet à un autre. Ces objets peuvent être définis informellement comme des conteneurs d'informations [27]. Le *flux d'informations* est généralement contrôlé par l'attribution d'une classe de sécurité (appelé aussi étiquette de sécurité) aux objets et aux sujets. Le passage de l'information d'un objet *x* à un objet *y* signifie l'existence d'un flux d'informations de la classe de sécurité de *x* à la classe de sécurité de *y*. Ce flux peut être réalisé par des opérations de lecture, écriture, ou leurs combinaisons.

Denning [27] définit le concept de politique de flux d'informations en considérant un triple $<SC, \rightarrow, \oplus>$ tel que :

- SC est un ensemble de *classes de sécurité*.
- $\rightarrow \subseteq SC \times SC$ est une relation binaire peut-*passer* dans SC.
- $\oplus : SC \times SC \rightarrow SC$ est un *opérateur de jointure* sur SC.

$A \rightarrow B$ signifie que l'information peut passer de la classe de sécurité A à la classe de sécurité B. L'opérateur de jointure permet de déterminer les étiquettes de sécurité des objets qui contiennent de l'information provenant de deux classes de sécurité. Ainsi, $A \oplus B = C$ signifie que les objets qui contiennent des informations provenant des classes de sécurité A et B doivent être étiquetés par la classe de sécurité C.

Dans le *contrôle d'accès basé sur les treillis* « *Lattice based access control* » (*LBAC*) [27, 83, 94, 11], un treillis est utilisé pour définir les niveaux de sécurité des objets et des sujets. Pour présenter ce contrôle d'accès nous commençons par la définition du concept : *ordre partiel*. Un *ordre partiel* est une relation binaire $\leq$ sur un ensemble P, qui est *réflexive*, *antisymétrique* et *transitive*. Ainsi, pour tout a, b et c dans P, nous avons ce qui suit :

- $a \leq a$ (ceci veut dire que la relation est réflexive),
- si $a \leq b$ et $b \leq a$ alors $a = b$ (ceci veut dire que la relation est antisymétrique),
- si $a \leq b$ et $b \leq c$ alors $a \leq c$ (ceci veut dire que la relation est transitive).

Une relation d'ordre partiel dans le contexte du contrôle d'accès est définie par :

- des *niveaux de sécurité H* avec des classifications linéaires $\leq$,
- des *catégories C* tels que les noms de projets, les divisions d'entreprise, etc.,
- des *étiquettes de sécurité* qui sont des paires *(h, c)* où $h \subseteq H$ et $c \subseteq C$.

Ainsi, une étiquette de sécurité dans *LBAC* est définie par la paire (niveau de sécurité, catégorie). Les paires d'étiquettes de sécurité peuvent être liées par la relation *dom* comme elles peuvent ne pas l'être, *dom* étant une relation d'ordre partiel définie comme suit :

(h1, c1) dom (h2, c2) si et seulement si $h1 \leq h2$ *et* $c1 \subseteq c2$

3.2.1 Modèle Bell-LaPadula

Parmi les modèles basés sur les treillis, le modèle *Bell-LaPadula* développé par *David Elliott Bell* et *Len LaPadula* [8] pour le département de la défense américaine, formalise la *sécurité multi-niveaux* et met l'accent sur la *confidentialité* des données. Dans ce

modèle, l'attribution des droits d'accès dépend des étiquettes de sécurité attribuées aux objets (*Classifications*) et aux sujets (*Habilitations*). Les règles obligatoires définies par ce modèle préviennent le flux d'information d'un haut niveau de confidentialité à un niveau de confidentialité plus bas. Le modèle *Bell-LaPadula* adopte une approche de contrôle d'accès en deux étapes qui consiste à :

1. définir une matrice d'accès discrétionnaire *D* [64] qui permet de déterminer les droits d'accès des sujets et dont le contenu peut être modifié par les sujets. Toutefois, une autorisation dans *D* n'est pas suffisante pour qu'un accès soit permis.
2. autoriser chaque accès seulement après la vérification de sa conformité à la politique de contrôle d'accès obligatoire.

Ce modèle est défini par deux propriétés qui doivent être satisfaites pour assurer la confidentialité des données : la *propriété simple* et la *propriété étoile*. Pour définir ces propriétés, nous supposons que les classifications et les habilitations sont comparables.

3.2.1.1 Propriété simple de Bell-LaPadula

La *propriété simple* peut être décrite tout simplement par la phrase « *ne pas lire en haut* ». En effet, cette propriété interdit à un sujet *s* d'accéder en lecture à un objet *o* qui a une classification $\gamma(o)$ plus élevée que son habilitation $\gamma(s)$. Autrement dit, un sujet *s* peut lire un objet *o* seulement si $\gamma(s) \geq \gamma(o)$.

3.2.1.2 Propriété étoile de Bell-LaPadula

La propriété étoile peut être décrite tout simplement par la phrase « *ne pas écrire en bas* ». En effet, cette propriété interdit à un sujet *s* d'accéder en *écriture* à un objet *o* qui a une classification $\gamma(o)$ moins élevée que son habilitation $\gamma(s)$. Autrement dit, un sujet *s* peut écrire dans un objet *o* seulement si $\gamma(s) \leq \gamma(o)$.

3.2.1.3 Principe de tranquillité

Afin d'interdire les flux d'informations non autorisés par les modèles de contrôle d'accès multi-niveaux, le principe de *tranquillité* interdit la modification des étiquettes de sécurité des sujets et des objets (sauf par l'administrateur). Ce principe peut être assoupli

de plusieurs manières. Certaines sont sécures et d'autres non sécures. Une modification des étiquettes de sécurité est dite non sécure lorsqu'elle provoque un flux d'information d'un haut niveau de confidentialité vers un niveau de confidentialité plus bas. Ainsi des informations confidentielles pourraient être divulguées.

3.2.1.4 Modèle du plus haut niveau

Le modèle du *plus haut niveau* (*High water mark*) [98] est antérieur à celui de *Bell-LaPadula*. Ce modèle se base sur les deux propriétés suivantes :

1. Lorsqu'un sujet lit un objet qui a niveau de confidentialité plus élevé, il est étiqueté avec le niveau de confidentialité de cet objet.
2. Lorsqu'un sujet écrit dans un objet qui a un niveau de confidentialité inférieur, l'objet est étiqueté avec le niveau de confidentialité du sujet.

3.2.1.5 Discussion

Le modèle de *Bell-LaPadula* permet seulement d'assurer l'objectif de sécurité de confidentialité et ne permet pas de créer de nouveaux sujets et objets. Il pourrait être impossible de l'appliquer dans certains cas à cause de sa rigidité puisque les règles obligatoires limitent le partage de l'information.

3.2.2 Modèle BIBA

Le modèle d'intégrité *Biba* [9], développé par Kenneth J. Biba en 1977 formalise la sécurité multi-niveaux et permet de garantir l'intégrité des données. En effet, il existe de nombreux systèmes dans lesquels il est essentiel d'éviter la modification de certaines données par des sujets non autorisés (les systèmes de réservation de vol, les systèmes d'informations médicales, etc.). Dans ce modèle, l'attributiondes accès dépend des niveaux d'intégrité attribués aux objets et aux sujets.

Le concept de base dans le modèle de *Biba* est que l'information à faible intégrité ne doit pas être autorisée à passer à des objets qui ont une intégrité élevée, alors que l'inverse est acceptable. Tout comme le modèle *Bell-LaPadula*, le modèle *Biba* est défini par deux propriétés : la propriété *simple* et la propriété *étoile*. Ces deux propriétés duales

des propriétés de *Bell-LaPadula*, doivent être satisfaites pour assurer l'intégrité des données.

3.2.2.1 Propriété simple de BIBA

La *propriété simple* peut être décrite tout simplement par la phrase « ne pas lire en bas ». En effet, cette propriété interdit à un sujet qui a un niveau d'intégrité $\varphi(s)$ d'accéder en lecture à un objet qui a un niveau d'intégrité $\varphi(o)$ tel que $\varphi(s) > \varphi(o)$.

3.2.2.2 Propriété étoile de BIBA

La *propriété étoile* peut être décrite tout simplement par la phrase « ne pas écrire en haut ». Cette propriété interdit à un sujetqui a un niveau d'intégrité $\varphi(s)$, d'accéder en écriture à un objet qui a un niveau d'intégrité $\varphi(s)$ tel que $\varphi(s) < \varphi(o)$.

3.2.2.3 Modèle du plus bas niveau

Le modèle du *plus bas niveau* (*Low water mark*) [8] est une extension du modèle de*Biba*. Ce modèle se base sur les deux propriétés suivantes :

1. Lorsqu'un sujet lit un objet qui a niveau d'intégrité moins élevé, il est étiqueté avec le niveau d'intégrité de cet objet.
2. Lorsqu'un sujet écrit dans un objet qui a un niveau d'intégrité plus élevé, l'objet est étiqueté avec le niveau d'intégrité du sujet.

3.2.2.4 Similitudes entre Bell-LaPadula et BIBA

Il n'ya pas de différence fondamentale entre le modèle *Biba* et le modèle *Bell-LaPadula*. Les deux modèles autorisent les flux d'information dans un sens seulement. Le modèle *Bell-LaPadula* autorise le flux d'information vers le haut et le modèle *Biba* l'autorise vers le bas. Un système qui peut appliquer l'un de ces modèles peut également appliquer l'autre puisque les règles d'accès dans les deux modèles se basent sur les étiquettes de sécurité des sujets et des objets. En effet, il suffit d'une reconfiguration simple de ces étiquettes ou l'inversement de la relation de dominance. Ces deux modèles peuvent être combinées dans des situations où la confidentialité et l'intégrité sont à assurer simultanément.

3.2.2.5 Discussion

Le modèle *Biba* ne permet pas d'assurer l'objectif de confidentialité et ne supporte pas l'octroi et le retrait des accès. Il est généralement impossible de l'appliquer dans plusieurs organisations à cause de sa rigidité.

3.2.3 Modèle de Brewer et Nash

Le modèle de *Brewer et Nash* [15] est un modèle de contrôle d'accès dynamique qui analyse l'historique des accès pour déterminer les décisions d'accès. Ce modèle, aussi appelé le modèle de la *muraille de Chine*, a été développé pour réduire les conflits d'intérêts dans des organisations commerciales et assurer l'objectif de confidentialité. Un conflit d'intérêts survient lorsqu'un sujet a accès aux informations confidentielles de deux organisations en compétition. Ce modèle introduit les concepts suivants :

- les *objets* qui appartiennent aux *organisations*,
- les *organisations* qui disposent de plusieurs objets utilisés dans le cadre de leurs activités,
- les *classes de conflits d'intérêts* qui regroupent des organisations qui sont en concurrence.

Ce modèle se base aussi sur deux propriétés : la *propriété simple* et la *propriété étoile*.

3.2.3.1 Propriété simple de Brewer et Nash

La *propriété simple* interdit l'accès d'un sujet en *lecture* à un objet si ce dernier appartient à une organisation appartenant à la même classe de conflit.

3.2.3.2 Propriété étoile de Brewer et Nash

La *propriété étoile* interdit l'accès d'un sujet en *écriture* à un objet si le sujet a déjà accédé en lecture à un objet d'une autre organisation.

3.2.3.3 Discussion

Le modèle de la *muraille de Chine* est simple et facile à décrire. Cependant, sa mise en œuvre est moins simple. En effet, la détection et l'élimination des canaux cachés sans

encourir de pénalités significatives de performance représentent un problème important. Ce modèle peut aussi être trop restrictif comme discuté dans [83].

3.3 Modèle de contrôle d'accès basé sur les rôles

Le *contrôle d'accès basé sur les rôles* [3, 34, 35, 36, 84] «*Role Based Access Control*» (*RBAC*) peut être considéré comme une approche alternative au *contrôle d'accès obligatoire* (MAC) et au *contrôle d'accès discrétionnaire* (*DAC*). Ce modèle est très utilisé en pratique. Il se compose de quatre modèles : *RBAC de base*, *RBAC hiérarchique*, *RBAC avec des contraintes statiques* et *RBAC avec des contraintes dynamiques*.

3.3.1 Modèles RBAC

Comme nous pouvons le voir dans la *Figure 2* [3], *RBAC de base* introduit cinq concepts : un ensemble d'*utilisateurs* (*USERS*), un ensemble de *rôles* (*ROLES)*, un ensemble d'*objets* (*OBS*), un ensemble d'opérations ou de *droits d'accès* (*OPS*) et un ensemble de *permissions* (*PRMS*).

Les rôles découlent généralement de la structure d'une organisation et sont des noms qui sont associés à des ensembles de permissions *(PRMS* $= 2^{(OPS \times OBS)}$*)*. Les permissions sont des ensembles de couples (*opération, objet*) et sont affectées aux rôles ($PA \subseteq PRMS \times ROLES$, est une relation *n-aire* d'affectation des permissions aux rôles). Les rôles sont affectés aux utilisateurs actifs dans une session ($UA \subseteq USERS \times ROLES$, est une relation n-aire d'affectation des rôles aux utilisateurs). Une session est une correspondance entre un utilisateur et un ensemble actif de rôles (*session_roles* retourne les rôles activés dans une session et *user_sessions* retourne l'utilisateur qui est associé à une session). Ce modèle est « idéal » pour les entreprises dont la fréquence de changement du personnel est élevée puisqu'il simplifie l'ajout ou la suppression des utilisateurs. Par exemple, dans le cas d'un gérant *Marc* remplacé par la gérante *Marie*, il n'est pas nécessaire d'affecter à *Marie* séparément toutes les permissions de *Marc* mais il suffit d'affecter à *Marie* le même rôle que *Marc*.

RBAC hiérarchique introduit le concept de la *hiérarchie des rôles* (*RH*), défini comme un ordre partiel sur les rôles, pour permettre l'héritage de permissions.

RBAC avec des contraintes statiques (séparation des tâches) permet d'ajouter de contraintes sur l'affectation des rôles. Exemple de contrainte statique **:** Un utilisateur ne peut pas avoir deux rôles en conflit d'intérêt.

RBAC avec des contraintes dynamiques permet d'ajouter des contraintes sur l'activation des rôles. Exemple de contrainte dynamique : Un utilisateur ne peut pas avoir deux rôles *actifs* en conflit d'intérêt.

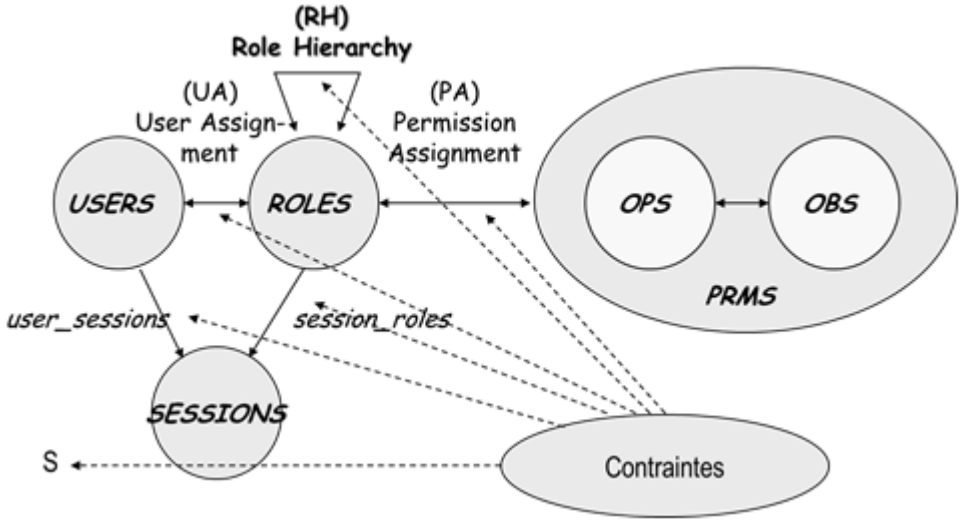


Figure 2. Concepts de RBAC [3]

3.3.2 Discussion

Les limitations suivantes caractérisent le modèle *RBAC* [36] :

- La définition et l'optimisation des rôles (*ingénierie des rôles*) dans une organisation est une tâche complexe à cause de la difficulté de trouver un compromis entre l'atteinte de l'objectif du *moindre privilège* qui nécessite une définition granulaire des rôles et la simplification de l'administration qui nécessite une diminution du nombre de rôles.
- La difficulté d'assurer la conformité de la hiérarchie implémentée à la hiérarchie des rôles.

- La difficulté de le mettre en œuvre et la nécessité dele combiner avec d'autres modèles de contrôle d'accès pour répondre aux besoins des organisations.
- La difficulté de contrôler les flux d'information.
- L'attribution des droits d'accès n'est pas à la discrétion des utilisateurs ce qui rend difficile l'implémentation des modèles d'accès discrétionnaires.

3.4 Contrôle d'accès basé sur les attributs

Le *contrôle d'accès basé sur les attributs* «*Attribute based access control*» (*ABAC*) [51] permet de déterminer les décisions d'accès en considérant les attributs des sujets (poste d'un employé, sa date d'embauche, sa localisation, etc.), des objets (emplacement physique, emplacement logique, etc.), des actions et des conditions de l'environnement (le temps de la requête, la température, la valeur de la menace de la requête, etc.) qui sont des facteurs dynamiques indépendants des sujets et des objets. Le langage utilisé généralement pour spécifier les politiques d'accès dans *ABAC* est le langage *XACML* [51].

Un *attribut* est une caractéristique prédéfinie et pré-attribuée qui définit un aspect spécifique des sujets, des objets, des actions demandées et des conditions de l'environnement. Les attributs ne sont pas nécessairement liés les uns aux autres et peuvent provenir de plusieurs sources. Il convient également de noter que le rôle d'un employé dans une organisation peut être considéré comme un attribut dans le modèle *ABAC*.

Une requête d'accès est un ensemble de couples *(attribut, valeur).*

Exemple : *Nom(sujet) = Michel, Age(sujet) = 30, Identif(action) = Écriture.*

Les étapes suivantes décrivent le processus de prise de décision du modèle *ABAC* :

1. Un sujet demande l'accès à un objet en présentant un ensemble de valeurs d'attributs.

Un exemple de politique est le suivant : l'accès est permis si *(Rôle(sujet) = Étudiant)* et *(Programme(sujet) = Doctorat)* et *(Identif(action) = lecture)* et *(Identif(ressource) = thèse).*

2. Le système de contrôle d'accès compare les valeurs des attributs des sujets et des objets et les valeurs des conditions de l'environnement aux valeurs définies par les politiques de contrôle d'accès qui sont des expressions booléennes qui définissent l'ensemble des opérations permises à un sujet sur un objet selon certaines valeurs des attributs.
3. Une décision d'accès (*permettre, refuser*) est déterminée.

3.4.1 Mécanismes de contrôle d'accès ABAC

Le modèle *ABAC* fournit une architecture décrite par la *Figure 3* [51] qui montre ses principaux points fonctionnels : le *point d'application de la politique* (*PEP*), le *point de décision de la politique* (*PDP*), le *point d'information de la politique* (*PIP*), et le *point d'administration de la politique* (*PAP*). Ces composants fonctionnent ensemble pour appliquer la politique de contrôle d'accès et fournir des décisions d'accès.

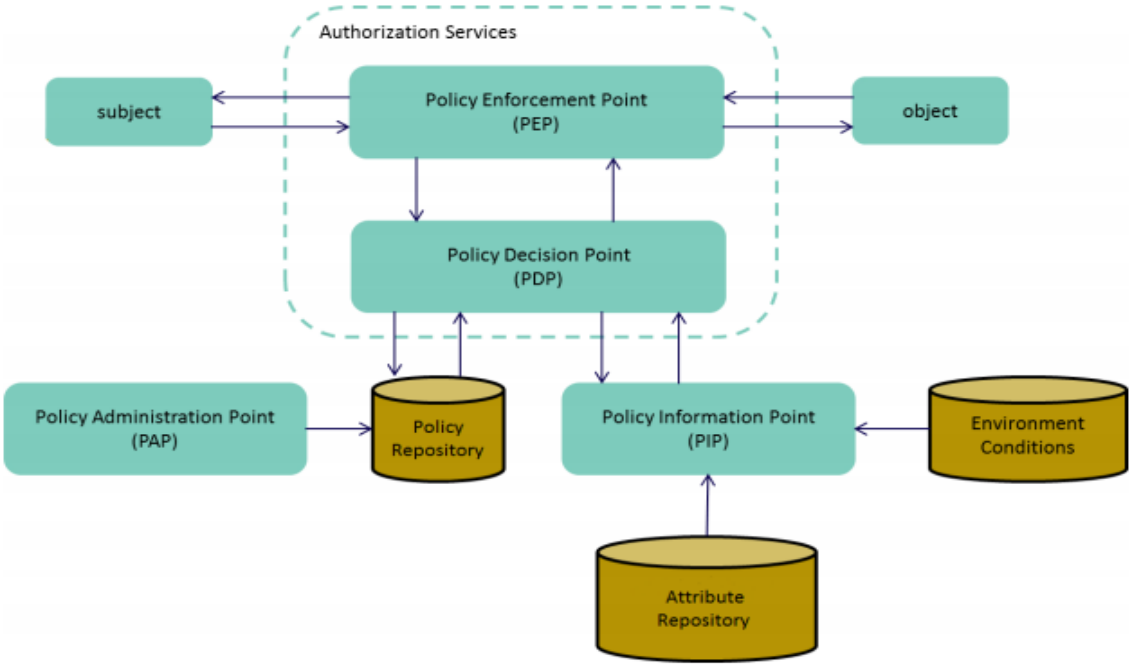


Figure 3. Points fonctionnels de ABAC [51]

Le *point de décision des politiques* ou *PDP* (*Policy Decision Point*) est l'entité qui sélectionne à partir du *dépôt des politiques* (*Policy repository*), les politiques qui sont applicables à une requête d'accès afin de déterminer une décision d'accès.

Le *point d'application des politiques* ou *PEP* (*Policy Enforcement Point*) est l'entité qui transmet la requête au *PDP* pour demander une réponse. Le *PEP* applique la décision d'accès transmise par le *PDP*.

Le *point d'information de la politique* ou *PIP* (*Policy Information Point*) fournit à partir du dépôt des attributs, les attributs et les conditions de l'environnement nécessaires au *PDP*.

Le *point d'administration de la politique* ou *PAP (Policy administration point)* fournit une interface utilisateur qui permet de créer, gérer, tester et déboguer les politiques.

3.4.2 Discussion

Le modèle *ABAC* offre la possibilité de contrôler l'accès sans prédéfinir une liste de sujets. Cela pourrait être d'un grand intérêt dans les grandes entreprises ayant un effectif qui change fréquemment. Une limitation du modèle *ABAC* est la difficulté d'uniformiser les attributs dans toutes les unités organisationnelles d'une entreprise.

3.5 Modèle de contrôle de l'usage

Le modèle de *contrôle de l'usage* « *Usage Control* » (*UCON*) [80] qui est un modèle de contrôle d'accès basé sur les attributs comporte les concepts suivants présentés par la *Figure 4* :

- les *sujets* (*Subjects*) et leurs *attributs* (*Subject attributes*),
- les *objets* (*Objects*) et leurs *attributs* (*Object attributes*),
- les *droits d'accès* (*Rights*),
- les *autorisations* (*Authorizations*) qui sont des prédicats définis en fonction des attributs,

- les *obligations* (*Obligations*) qui sont des activités qui doivent être réalisées avant ou lors d'un accès,
- les *conditions* (*Conditions*) qui sont les restrictions sur le système ou l'environnement imposées avant ou pendant un accès.

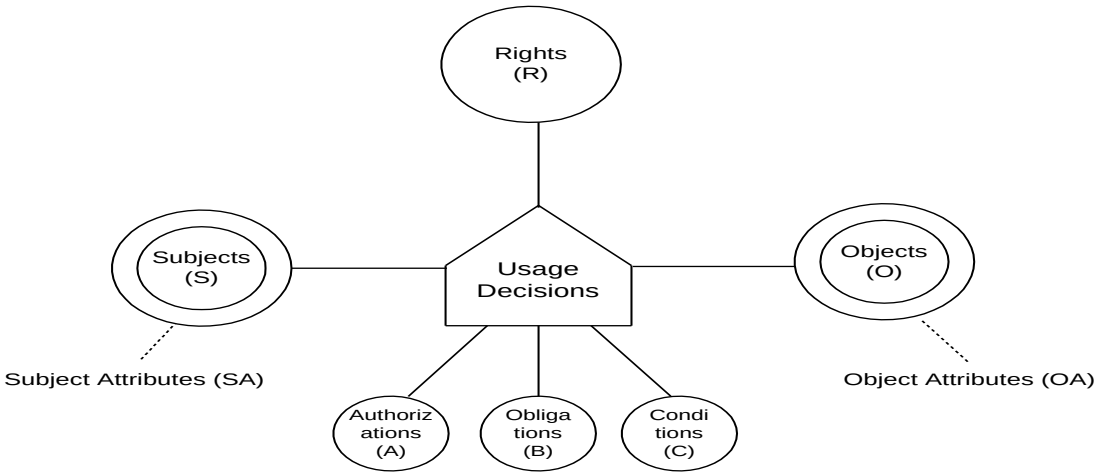


Figure 4. Concepts de UCON [80]

3.5.1 Caractéristiques du modèle de contrôle d'usage

Comme nous pouvons le voir dans la *Figure 5* [59], les propriétés qui distinguent le modèle *UCON* des modèles traditionnels de contrôle d'accès sont les suivantes :

- un *processus* de trois phases pour la prise des décisions d'accès,
- la *continuité des décisions* d'accès ce qui signifie que ces décisions peuvent être déterminées et appliquées non seulement avant un accès, mais aussi pendant l'accès,
- la *mutabilité des attributs* qui signifie que les attributs des sujets et des objets peuvent être mis à jour même suite à un accès.

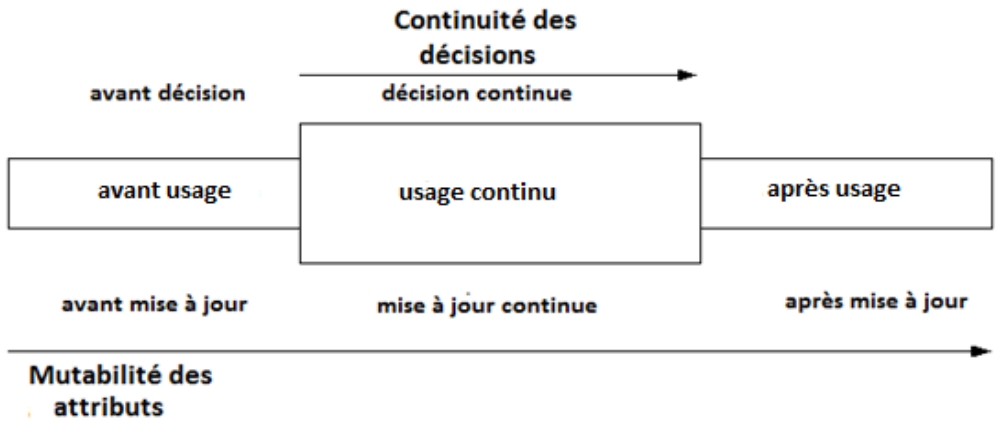


Figure 5. Continuité des décisions et mutabilité des attributs [59]

Selon les points de mise à jour de l'attribut d'accès, nous avons sept modèles d'autorisation de base:

- *preA0* : la décision d'accès est déterminée avant l'accès, et les attributs ne sont pas mis à jour.
- *preA1* : la décision d'accès et les attributs sont mis à jour avant l'accès.
- *preA2* : la décision d'accès est déterminée avant l'accès et les attributs sont mis à jour après l'accès.
- *onA0* : la décision d'accès est déterminée et vérifiée lors de l'usage et les attributs ne sont pas mis à jour.
- *onA1* : la décision d'accès est déterminée et vérifiée lors de l'usage et les attributs sont mis à jour avant l'accès.
- *onA2* : la décision d'accès est déterminée et vérifiée lors de l'usage et les attributs sont mis à jour lors de l'usage.
- *onA3* : la décision d'accès est déterminée et vérifiée lors de l'usage et les attributs sont mis à jour après l'usage.

3.5.2 Discussion

Le modèle *UCON* permet d'éviter les limites des modèles de control d'accès traditionnels comme le montre le *Tableau 1* :

UCON	***Modèles de contrôle d'accès traditionnels***
Contrôle d'accès basé sur les obligations et les conditions	*Contrôle d'accès basé sur l'autorisation*
Basé sur les attributs	*Basé sur les identités*
Contrôle d'accès continu	*Décision d'accès avant accès*
Attributs mutables	*Attributs non mutables*
Droits d'accès dynamiques	*Droits d'accès prédéfinis et attribués à des sujets*

Tableau 1. Tableau comparatif entre UCON et le contrôle d'accès traditionnel

Cela dit, le modèle *UCON* est difficile à implémenter et à notre connaissance n'a pas été encore l'objet d'une utilisation commerciale.

3.6 Conclusion

Dans ce chapitre, nous avons présenté un ensemble des modèles de contrôle d'accès les plus connus dans la littérature. Chacun de ces modèles a été l'objet d'études approfondies pour des dizaines d'années et il a donc été impossible d'en donner plus qu'une description générale, cependant nous nous sommes limités à la description de concepts nécessaires pour la compréhension des idées de cette thèse. De plus, nous avons présenté les extensions de certains de ces modèles qui permettent de définir une politique d'accès moins restrictive et plus générale. Ces modèles accordent généralement les droits d'accès selon le principe du *besoin d'en connaître* (*Need to know*). Dans certains cas, ces modèles ne permettent pas de répondre aux besoins réels des organisations. Un contrôle d'accès flexible basé sur le risque qui permet de déroger aux politiques d'accès de façon sécuritaire pourrait être d'un grand intérêt. Dans le chapitre suivant, nous présentons des modèles qui intègrent la considération du risque à certains de ces modèles traditionnels.

Chapitre 4. État de l'art 2 : Méthodes de contrôle d'accès basées sur le risque

4.1 Introduction

Les systèmes de contrôle d'accès basés sur le risque étendent les concepts de contrôle d'accès traditionnels pour faciliter le partage de l'information. Ces systèmes permettent de prendre des décisions d'accès en tenant compte du risque. Toutefois, la détermination des risques d'accès est une tâche complexe, qui nécessite la considération de plusieurs facteurs tels que la fiabilité des sujets, la sensibilité des données, l'action demandée, l'historique des accès, l'emplacement physique ou l'emplacement logique à partir duquel l'accès est demandé, etc.

Dans ce chapitre, nous présentons un ensemble de travaux qui ont influencé directement ou indirectement notre recherche :

- le modèle de *contrôle d'accès adaptable basé sur le risque RADAC* [69] qui consiste à accorder ou refuser un accès en se basant sur le calcul du risque de sécurité et le calcul du besoin opérationnel,
- une approche qui permet de spécifier les principes de *RADAC* en utilisant le contrôle d'accès basé sur les attributs *ABAC* [59],
- une méthode qui permet d'estimer qualitativement le risque de dérogation aux politiques d'accès dans *RBAC* [7],
- quatre modèles [19] qui intègrent les concepts du risque dans le modèle *RBAC*,
- le modèle *MLS flou* [20] qui est le modèle de contrôle d'accès utilisé pour gérer les accès aux informations du *système S d'IBM* [52],
- un modèle de contrôle d'accès pour la protection des renseignements personnels des patients dans les systèmes d'informations de santé [96],
- un *système d'inférence floue* [77] (*Fuzzy inference system*) pour les systèmes de contrôle d'accès basés sur les risques.

Dans la section 4.9 de ce chapitre, nous présentons brièvement d'autres travaux, en lien avec l'évaluation du risque dans les systèmes de contrôle d'accès, que nous avons décidé de ne pas les présenter en détail en raison de contraintes d'espace.

4.2 Contrôle d'accès adaptable basé sur le risque (RADAC)

McGraw [69] présente le contrôle d'accès adaptable basé sur le risque (*Risk adaptabale access control RADAC*) qui consiste à accorder ou refuser un accès en se basant sur le calcul du *risque de sécurité* et le calcul du *besoin opérationnel*. Pour déterminer le risque de sécurité et les besoins opérationnels avant chaque décision d'accès plusieurs facteurs sont considérés :

- le niveau de confiance du demandeur d'accès,
- la sensibilité de l'information à accéder,
- la protection qui peut être accordée à l'information suite à une permission,
- le rôle du demandeur d'accès,
- l'importance de l'information pour une opération,
- l'incertitude,
- l'historique des décisions d'accès.

Les politiques de l'organisation sont utilisées pour établir les seuils de risques de sécurité et les seuils de besoins opérationnels.

4.2.1 Processus RADAC

Une requête d'accès à un objet déclenche le processus *RADAC* représenté par la *Figure 6*.

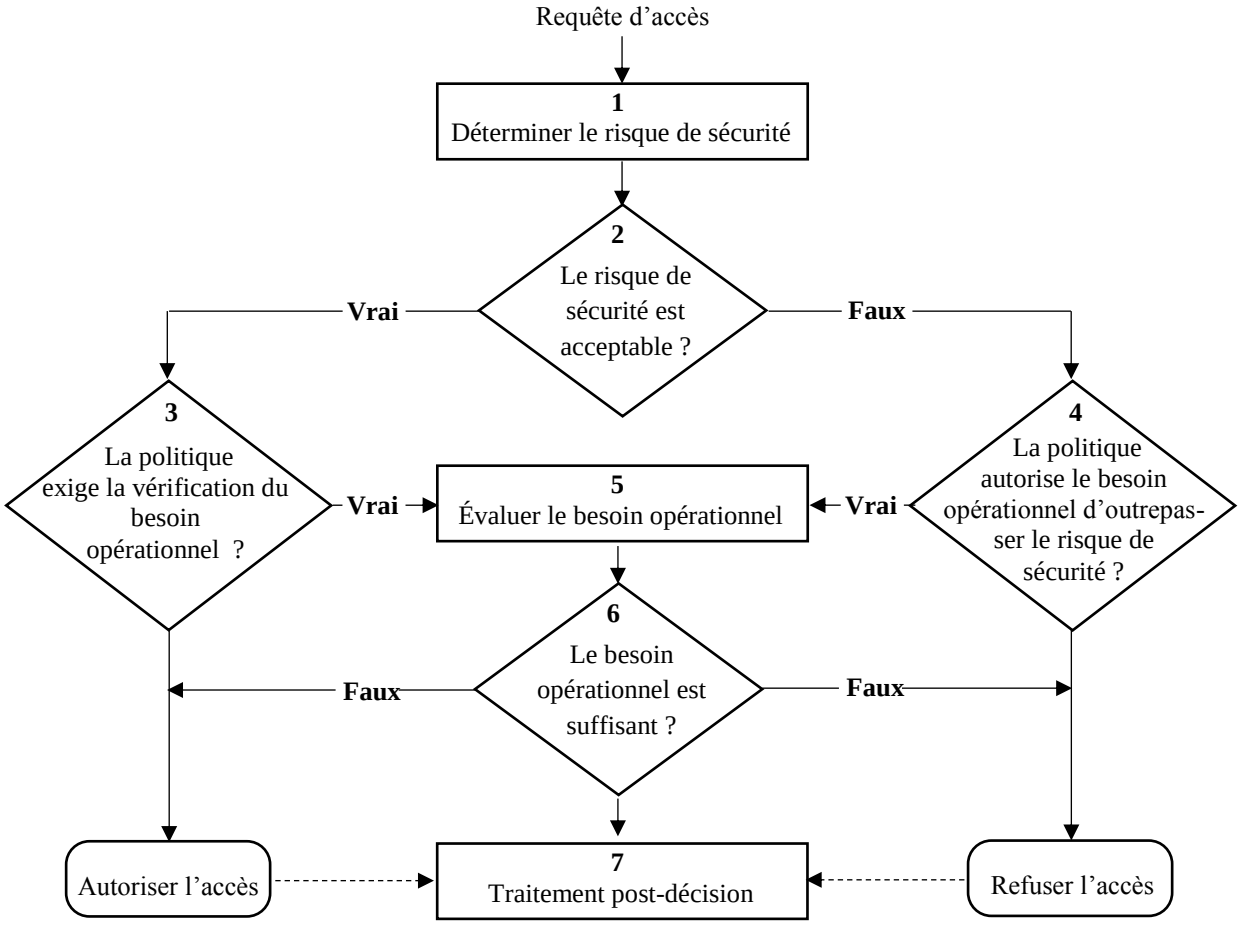


Figure 6. Processus RADAC (adapté de [69])

Le processus *RADAC* consiste à suivre les étapes suivantes :

4.2.1.1 Détermination du risque de sécurité

Le résultat de cette étape du processus *RADAC* est une estimation quantitative probabiliste, en temps réel, du risque de sécurité associé à l'octroi d'un accès demandé. Cette estimation est basée sur l'analyse de plusieurs facteurs (les utilisateurs, les composantes informatiques et l'environnement).

4.2.1.2 Comparaison du risque de sécurité à la valeur du risque acceptable

La valeur du risque de sécurité déterminée à l'étape précédente est comparée avec le *niveau de risque acceptable* de chaque domaine (les utilisateurs, les composantes

informatiques, etc.). Ces niveaux de risque acceptables sont définis dans la politique de contrôle d'accès.

4.2.1.3 Détermination de la nécessité de la vérification du besoin opérationnel

Cette étape permet de décider de la nécessité de la vérification du *besoin opérationnel*. Lorsque la politique exige cette vérification, un traitement supplémentaire est nécessaire (voir *4.2.1.5*). Autrement, l'accès est accordé.

4.2.1.4 Autorisation du besoin opérationnel à outrepasser le risque de sécurité

Dans le cas où le risque de sécurité est jugé inacceptable dans un ou plusieurs domaines, le besoin opérationnel doit être évalué pour décider de la possibilité d'outrepasser le risque de sécurité (voir *2.1.5*). Dans le cas contraire, l'accès est refusé.

4.2.1.5 Évaluation du besoin opérationnel

Au cours de cette étape, plusieurs facteurs sont analysés afin de déterminer si le demandeur a un besoin opérationnel suffisant pour accéder à l'information demandée. La politique précise des exigences différentes pour déterminer le besoin opérationnel à savoir l'appartenance du demandeur à une direction, son emplacement et sa position. Une autorisation d'un supérieur hiérarchique ou un service automatisé pourraient être requis pour témoigner de l'importance de l'accès pour l'accomplissement des tâches du demandeur. Un processus de flux de travail externe pourrait être utilisé pour obtenir cette approbation.

4.2.1.6 Vérification de la satisfaction des critères prédéterminés pour le besoin opérationnel

Cette étape consiste à déterminer si toutes les exigences définies dans la politique de sécurité, concernant le besoin opérationnel, sont satisfaites. Ainsi, l'accès est accordé si toutes les conditions sont remplies, et refusé dans le cas contraire.

4.2.1.7 Préparation du traitement post-décision

Au cours de cette étape, la décision déterminée, la justification de la décision et toute autre information pertinente sont analysées et sauvegardées. L'analyse des résultats sera effectuée automatiquement et en temps réel. Les résultats des décisions de contrôle

d’accès seront mis à la disposition des détenteurs de l’information et des administrateurs de sécurité pour les aider à évaluer et ajuster les politiques de contrôle d’accès.

4.2.1.8 Discussion

Le travail présenté, dans cette section, introduit une approche qui permet d’estimer le risque de sécurité associé à une requête d’accès, évaluer le besoin opérationnel de la requête et ajuster les politiques de contrôle d’accès. Cependant cette approche ne précise pas comment :

1. caractériser et paramétrer le besoin opérationnel afin que le processus *RADAC* puisse l’exploiter,
2. estimer le risque de chaque décision d’accès,
3. évaluer la confiance des personnes,
4. estimer la confiance des composants et des systèmes informatiques,
5. déterminer l’emplacement des composants informatiques et quantifier la menace à cet emplacement,
6. révoquer l’accès à l’information,
7. assurer la disponibilité de toutes les données qui seraient nécessaires pour prendre une décision basée sur le risque.

Nous verrons dans cette thèse que l’approche, que nous proposons, est plus spécifique par rapport aux points *2*, *3*, *4* et *5*.

4.3 Approche basée sur les attributs pour les modèles d’accès basés sur le risque

Kandala et al. [59] présentent une approche qui montre que, moyennant des extensions appropriées, il est possible d’interpréter les principes de *RADAC* [69] en utilisant les modèles de contrôle d’accès basés sur les attributs tels que *UCON* [80].

4.3.1 Modèle RADAC abstrait

La principale contribution de ce travailconsiste à spécifier un cadre formel afin de développer des modèles abstraits pour *RADAC* [69]. Les composants nécessaires pour modéliser *RADAC* sont représentés dans la *Figure 7*. (Dans la *Figure 7*, une flèche avec une seule pointe indique une relation qui a un élément pointé par la flèche alors que deux pointes indiquent une relation qui a plusieurs éléments pointés par la flèche. Cela permet de distinguer visuellement les relations *un à un*, *un à plusieurs* et *plusieurs-à-plusieurs*).

Les composants de base nécessaires pour modéliser *RADAC* sont comme suit : les *utilisateurs*, les *dispositifs*, les *finalités*, les *objets*, les *opérations*, les *connexions*, les *sessions* et les *facteurs situationnels locaux* et *globaux*. Les *utilisateurs*, les *dispositifs*, les *objets*, les *finalités*, *les opérations* et les *connexions* ont des attributs qui sont des propriétés utilisées pour prendre les décisions d'accès.

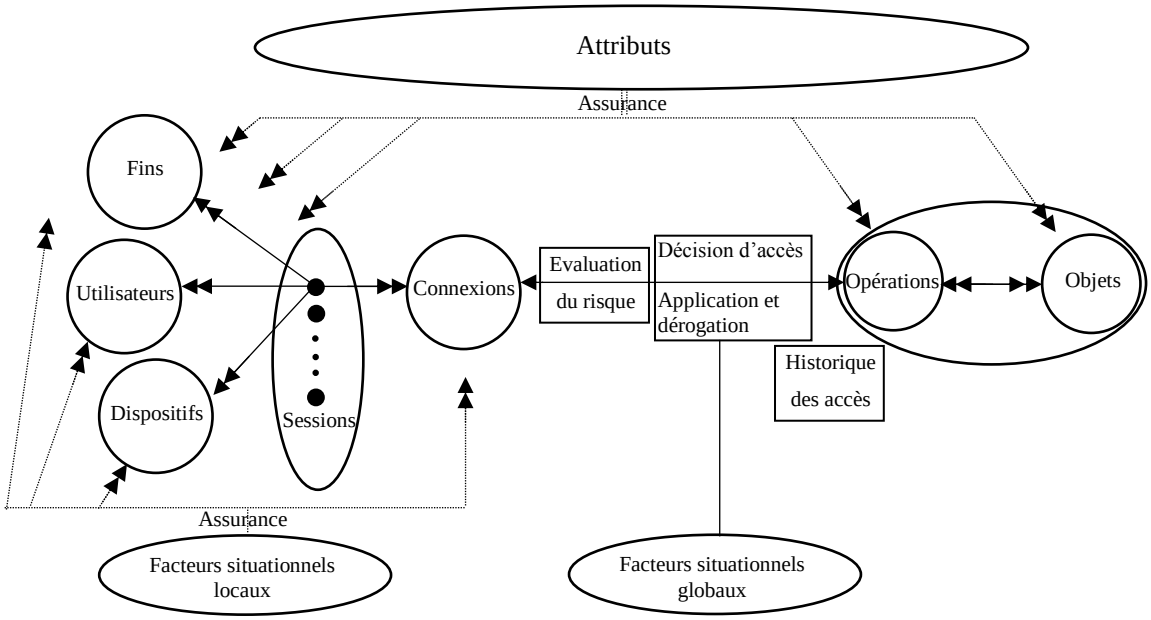


Figure 7. Composants RADAC (adapté de [59])

Dans ce qui suit, nous présentons des définitions nécessaires pour la compréhension de ce modèle :

Définition 1 : *U, D, OBS, OPS, C, P* et *S* représentent respectivement les *utilisateurs*, les *dispositifs*, les *objets*, les *opérations*, les *connexions*, les *finalités* et les *sessions*. Les facteurs situationnels sont des prédicats qui s'évaluent à vrai ou faux.

Une session est définie par un tuple $<u_i, d_j, p_k, c_l>$ où $u_i \in U$, $d_j \in D$, pk $\in 2^P$ et $c_l \in 2^C$. Autrement dit, une session est associée à un seul utilisateur et un seul dispositif, mais peut être associée à plusieurs *finalités* (*purposes*) et plusieurs connexions.

Pour formaliser les définitions d'attributs, une algèbre $\sum$ est utilisée. Cette algèbre est constituée des éléments suivants : un nom *a* pour désigner un attribut, une valeur d'attribut *v* appartenant à un domaine notée *dom(a)*, une identité du fournisseur d'attribut a_p et un niveau d'assurance l_{oa}.

UA, DA, CA, PA, OPA et *OBA* sont respectivement les attributs des *utilisateurs*, des *dispositifs*, des *connexions*, des *finalités*, des *opérations* et des *objets*. Chaque élément de ces ensembles est un tuple (a_p, *a*, *v*, l_{oa}) qui contient l'identité du fournisseur de l'attribut, le nom de l'attribut, la valeur de l'attribut et le niveau d'assurance.

Définition 2 : Une *demande d'accès* est représentée par $R \equiv \{ (a_{p1}; a_1; v_1; l_{oa1}), (a_{p2}; a_2; v_2; l_{oa2}), ... (a_{pk}; a_k; v_k; l_{oak})$ où $(a_{pi}; a_i; v_i; l_{oai}) \in UA \cup DA \cup CA \cup PA \cup OPA \cup OBA$ pour $1 \leq i \leq k$ }. Autrement dit, une demande d'accès est représentée par un ensemble de *tuples* où chaque tuple contient l'identité du fournisseur d'attribut, le nom de l'attribut, la valeur de l'attribut et le niveau d'assurance.

Définition 3 : Une *politique P* est une fonction $P : R \rightarrow E$. *R* représente le domaine des requêtes et *E* représente le domaine des décisions où *E* = {*permettre (permit), refuser (deny)*}.

Définition 4 : Une *fonction de décision d'accès ADF()* applique toutes les politiques de contrôle d'accès à une requête d'accès et retourne une décision d'accès. La fonction *ADF()* utilise un algorithme *combine_f()* qui combine les résultats de décisions renvoyées par la fonction de décision d'accès de chaque politique et retourne une décision d'accès finale. Une requête d'accès est autorisée si la décision d'accès finale est permise et refusée autrement. Formellement, *ADF(r) = combine_f {ADF(P1(r)), ADF(P2(r)), ADF(Pm(r))} = {permit; deny}.*

Définition 5 : *ObjectAccessHistory* est une fonction qui retourne l'historique des demandes d'accès passées, les attributs des demandes d'accès et les décisions d'accès. La fonction d'évaluation de risque prend en argument la requête et son historique d'accès et retourne la valeur du risque. La valeur du risque *rv* d'une requête est définie comme suit : *rv(r1) = RiskEvaluationFunction (r1, ObjectAccessHistory(r1)).*

Exemple : considérons une politique de contrôle d'accès obligatoire (*MAC*) modifiée [65]. La demande d'un utilisateur de lire un objet classé, est autorisée seulement si :

- l'habilitation de l'utilisateur est supérieure ou égale à la classification de l'objet,
- l'utilisateur a un besoin d'en connaître documenté pour accéder à cet objet,
- le niveau de *INFOCON* (un système de niveaux de menace aux États-Unis) est égale à *3, 4* ou *5*,
- le niveau de *DEFCON* (un état d'alerte utilisé par les forces armées des États-Unis) est égal à *3, 2* ou *1*.

Dans cet exemple, la condition concernant le niveau de risque acceptable exige que le risque d'une requête soit inférieur à une valeur spécifiée x_1. La détermination du niveau de risque tient compte de facteurs tels que le dispositif de l'utilisateur (dispositif sécurisé ou non), l'installation de l'endroit à partir duquel l'utilisateur demande l'accès (installation sécurisée ou installation inconnue), la localisation de l'utilisateur et l'historique des requêtes. La politique *P1* peut être exprimée de la façon suivante où *r* est une requête $(a_{p1};\ a_1;\ v_1;\ l_{oa1})$, $(a_{p2};\ a_2;\ v_2;\ l_{oa2})$, $(a_{p3};\ a_3;\ v_3;\ l_{oa3})$ *avec* a_1 = *RiskEvaluationFunction,* a_2 = *SubClearance et* a_3 = *ObjClassification :*

$$\mathrm{P1(r)} = \begin{cases} permit: \\ if \\ RiskEvaluationFunction(r) \leq x1 \wedge \\ operation = read \wedge \\ INFOCONLevel \leq 3 \wedge \\ DEFCONLevel \geq 3 \wedge \\ (SubClearance(r) \geq ObjClassification(r)) \\ deny: \\ Otherwise \end{cases}$$

4.3.2 Interprétation du modèle RADAC avec UCON

Ce travail montre qu'il est possible d'interpréter *RADAC* en utilisant des modèles de contrôle d'accès basé sur les attributs tels qu'*UCON*.

4.3.2.1 Points à considérer

Pour interpréter *RADAC* en utilisant *UCON*, les points suivants doivent être pris en considération :

- la définition du sujet,
- l'historique des accès,
- l'évaluation des risques.

Définition du sujet

Dans le modèle *UCON*, un sujet est un utilisateur humain qui a des attributs. Pour pouvoir capter les composants de *RADAC*, cette définition générale est décomposée en un ensemble de composants à savoir les *utilisateur*s, le *dispositif*, la *finalité* et la *connexion*.

Historique d'accès

Une caractéristique importante de *RADAC* consiste à considérer les décisions de contrôle d'accès précédentes. Cette caractéristique n'est pas prise en compte par *UCON* mais elle peut être partiellement capturée par le concept des attributs mutables.

Évaluation du risque

Pour déterminer une décision d'accès, le modèle *UCON* compare les attributs nécessaires et leurs valeurs alors que *RADAC* évalue le risque avant de déterminer une décision d'accès. Ainsi, l'évaluation du risque est intégrée à *UCON*.

4.3.2.2 Composants RADAC dans le modèle UCON étendu

Les composants de *RADAC* peuvent être interprétés par le modèle *UCON* étendu comme nous pouvons le voir dans la *Figure 8* :

- *UCON* définit un sujet comme un utilisateur humain qui a plusieurs attributs. Ainsi, ce concept d'*UCON* est décomposé en plusieurs concepts : les dispositifs, les utilisateurs, les fins, les objets et les connexions.
- Les facteurs situationnels dans *RADAC* peuvent être capturés par les conditions dans *UCON*.
- Les facteurs situationnels locaux de *RADAC* peuvent être exprimés par des attributs.
- Les opérations dans *RADAC* sont similaires aux droits d'accès dans *UCON*.
- La composante *application de la décision* dans *RADAC* est similaire aux autorisations et aux décisions d'utilisation dans *UCON*.
- Les fonctions de l'évaluation des risques et d'histoire d'accès dans *RADAC* font partie de la composante *autorisation* dans *UCON*.

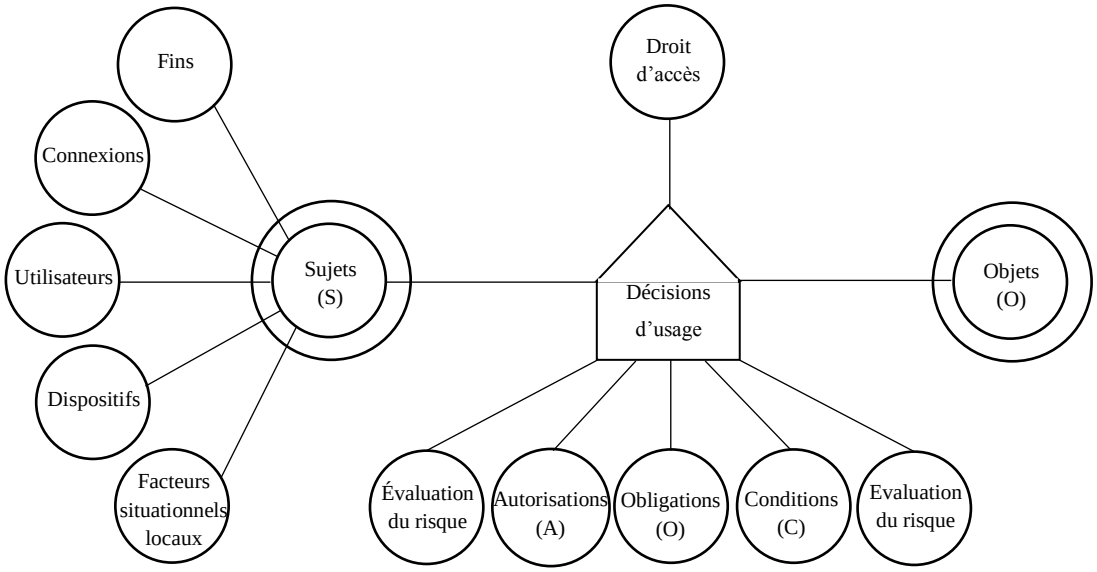


Figure 8. Composants RADAC dans le modèle UCON étendu (adapté de [59])

4.3.3 Extension des concepts de UCON à RADAC

Les concepts de mutabilité des attributs et la continuité de la prise de décision d'*UCON* peuvent enrichir *RADAC*. En effet, pour maintenir la continuité de la décision, l'évaluation des risques et des facteurs situationnels doivent être surveillés pendant la durée d'un accès afin d'assurer que les conditions d'accès soient toujours satisfaites.

4.3.4 Discussion

Ce travail [59] montre qu'il est possible d'interpréter le modèle *RADAC* avec le modèle *UCON étendu*. Cependant, ce travail n'inclut pas l'architecture, les détails de mise en œuvre de l'approche présentée, les protocoles et les mécanismes. Nous verrons dans cette thèse que notre approche utilise la mutabilité des attributs dans *ABAC* pour tenir compte de l'historique des accès et pour calculer le risque des requêtes.

4.4 Méthode d'estimation qualitative du risque de dérogation aux politiques d'accès

Dans *RBAC* [36], les accès sont accordés selon le principe du *besoin d'en connaître* (Need to know). Dans certains cas, ces accès accordés ne permettent pas de répondre aux besoins réels, d'où la nécessité de déroger aux politiques d'accès. Dans ce travail, *Bartsch* [7] propose une méthode qui permet d'estimer qualitativement le risque de dérogation aux politiques d'accès dans *RBAC*.

La *Figure 9* représente ce qui suit :

- une zone, limitée par les pointillés, qui représente les besoins d'accès réels (*Actual needs*),
- une zone en gris clair, contenue dans la zone limitée par les pointillés, qui représente les besoins identifiés pour les tâches routinières (*Identified needs for daily routine*),
- une zone en blanc qui représente les permissions par défaut (*Default permissions*),
- une zone en gris clair qui représente les actions ou les données dont il est possible de déroger à leurs politiques de sécurité (*Override actions or data*),
- une zone en gris foncé qui représente les actions ou les données qui ont un niveau de risque élevé (*Actions or data deemed too risky*),

- une *limite douce* (*Soft boundary*) dérivée de l'évaluation du besoin de savoir, qui sépare les permissions par défaut (la zone blanche) et les permissions qui peuvent être octroyées par la politique de dérogation,
- une *limite dure* (*Hard boundary*) qui détermine la limite des accès attribués par la politique de dérogation (l'espace au-delà de la *limite dure* représente un risque très élevé),
- une flèche qui montre que le niveau de risque augmente en allant de gauche à droite (*Increasing risk level*).

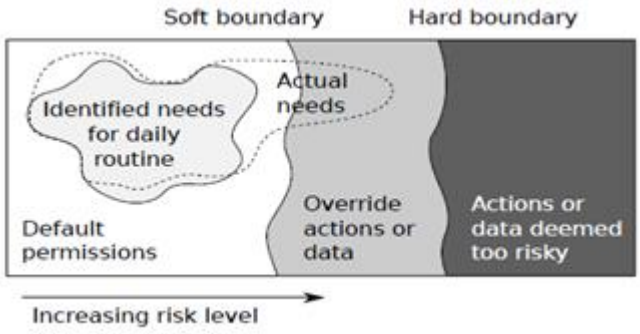


Figure 9. Limite dure et limite douce [7]

4.4.1 Estimation du risque

Ce travail propose des formules basées sur des principes de gestion des risques. La fonction ci-dessous permet d'estimer le risque d'une dérogation aux politiques d'accès. Cette fonction prend en argument le rôle et l'étendue de la dérogation (*extent)* qui représente les privilèges à ajouter à un rôle dans le cadre de cette dérogation.

Risk (role, extent) =
α (SpecificRisk (Confidentiality, role, extent),
SpecificRisk (Integrity, role, extent),
SpecificRisk (Availability, role, extent))

Le *risque* est égal à la valeur maximale (dénotée par *α*) des risques spécifiques. Un risque spécifique est le risque pour chaque objectif de sécurité (confidentialité, intégrité et disponibilité).

Pour chaque objectif de sécurité (confidentialité, intégrité et disponibilité), le *risque spécifique SpecificRisk* est estimé par la fonction suivante :

SpecificRisk (objective; role; extent) =
ThreatLikelihood(objective; role; extent) ⊗ ProtectionNeed(objective; extent)

L'opérateur ⊗ est défini par la matrice représentée par le tableau ci-dessous :

⊗		***Besoin de protection***		
		Normal (N)	*Élevé (É)*	*Très élevé (T)*
Probabilité de la menace	*Normal (N)*	*N*	*N*	*T*
	Élevé (É)	*N*	*É*	*T*
	Très élevé (T)	*N*	*É*	*T*

Tableau 2. Risque spécifique

Un *risque spécifique* est évalué en évaluant le *besoin de protection* (*ProtectionNeed)* et la *probabilité de la menace* (*ThreatLikelihood)*. Le besoin de protection est déterminé par l'évaluation de l'impact de la perte de confidentialité, d'intégrité ou de disponibilité. La *probabilité de la menace* (*ThreatLikelihood),* définie comme la probabilité de la survenance d'un incident, est évaluée en utilisant la fonction ci-dessous :

ThreatLikelihood(objective; role; extent) =
RoleThreat(role) ⊙ OpportunityThreat (objective; extent)

L'opérateur ⊙ est défini par une matrice représentée par le *Tableau 3*.

⊙		***Menace du rôle***		
		Normal (N)	*Élevé (É)*	*Trèsélevé (T)*
Opportunité	*Normal (N)*	*N*	*É*	*T*
	Élevé (É)	*N*	*T*	*T*
	Très élevé (T)	*É*	*T*	*T*

Tableau 3. Probabilité de la menace

Deux critères sont considérés pour estimer la probabilité de la menace :

- La *menace du rôle* induite par les caractéristiques personnelles *des* utilisateurs (*RoleThreat)* qui permet d'évaluer à quel point un groupe d'employés est fiable pour un rôle donné.
- La *menace d'opportunité* (*OpportunityThreat)* qui représente la tentation causée par l'attribution du nouveau privilège en cas de dérogation. Les facteurs

considérés pour évaluer ce critère sont : le niveau de fiabilité des employés, leur niveau de satisfaction, leurs antécédents, etc.

4.4.2 Estimation du bénéfice

Bien qu'il existe des risques potentiels suite à la dérogation aux politiques d'accès, une entreprise peut bénéficier de la flexibilité des décisions d'accès qu'elle offre. Les bénéfices sont estimés avec la fonction suivante :

Benefit(role; extent) =
Frequency(role) × BenefitPerOverride(role; extent)

L'opérateur × est défini par une matrice représentée par le *Tableau 4*.

×		***Fréquence des dérogations par rôle***		
		Normal (N)	*Élevé (É)*	*Très élevé (T)*
Bénéfice par dérogation	*Normal (N)*	*N*	*É*	*É*
	Élevé (É)	*É*	*É*	*T*
	Très élevé (T)	*É*	*T*	*T*

Tableau 4. Bénéfice

Le *bénéfice* est estimé à partir des deux facteurs suivants :

- la *fréquence des dérogations* (*Frequency)* qui représente la fréquence des situations où des dérogations à la politique d'accès sont nécessaires pour chaque rôle,
- le *bénéfice par dérogation* (*BenefitPerOverride)* qui pourrait être réalisé.

Chaque dérogation à la politique d'accès apporte un bénéfice mais engendre également des efforts d'audit. Ainsi, le bénéfice par dérogation est évalué en utilisant la fonction ci-dessous :

BenefitPerOverride (role; extent) = EfficiencyGainPerOverride(role; extent) - EffortPerOverride

Les résultats de l'opérateur – sont déterminés par la matrice représentée par le *Tableau 5*.

-		***Effort par dérogation***		
		Normal (N)	*Élevé (É)*	*Trèsélevé (T)*
Gain par dérogation	*Normal (N)*	*N*	*É*	*É*
	Élevé (É)	*É*	*É*	*T*
	Très élevé (T)	*É*	*T*	*T*

Tableau 5. Bénéfice par dérogation

Deux facteurs sont considérés pour estimer le bénéfice par dérogation :

- le gain par dérogation (e*fficiencyGainPerOverride)* qui est évalué séparément pour chaque rôle,
- l'effort par dérogation (*EffortPerOverride)* qui représente l'effort additionnel que l'entreprise doit investir par dérogation et qui est causé surtout par la nécessité d'auditer les actions effectuées dans le cadre de la dérogation.

4.4.3 Pertinence de la dérogation

La fonction ci-dessous permet d'évaluer la pertinence de la dérogation *(OverrideAdequacy)* qui aide à décider concernant l'attribution des actions additionnelles aux rôles et la dérogation aux politiques d'accès.

OverrideAdequacy(role; extent) =
Risk (role; extent) ⋈ *Benefit(role; extent)*

L'opérateur ⋈ balance le *risque* avec le *bénéfice*. L'interprétation des résultats de cet opérateur dépend du niveau de risque acceptable de l'organisation.

Le tableau ci-dessous représente le résultat de la fonction *OverrideAdequacy.*

⋈		***Risque***		
		Normal	*Élevé*	*Trèsélevé*
Bénéfice	*Normal*	*N*	*F*	*F*
	Élevé	*É*	*N*	*F*
	Très élevé	*T*	*T*	*N*

Tableau 6. Pertinence de la dérogation

Les résultats présentés dans le *Tableau 6,* sont obtenus en affectant les valeurs *1*, *2* et *3* respectivement aux niveaux de risque, *normal* (*Normal*), *élevé* (*High*) et *très élevé* (*Very High*). Le résultat du rapport *bénéfice / risque* est interprété comme suit :

faible (F) lorsque les valeurs $a < 1$, *Normal(N)* lorsque $1 \leq a < 1{,}5$, *Élevé (É)* lorsque $1 \leq a < 1{,}5$ et *Très élevé (T)* lorsque $a \geq 2{,}5$.

Le résultat de cet opérateur ne permet pas une évaluation absolue de la pertinence de la dérogation mais aide à déterminer un *ordre de priorité* des combinaisons *rôle/ privilège additionnel*.

La *Figure 10* est une représentation graphique des différentes étapes suivies pour évaluer la pertinence de la dérogation selon l'approche présentée par Bartsh.

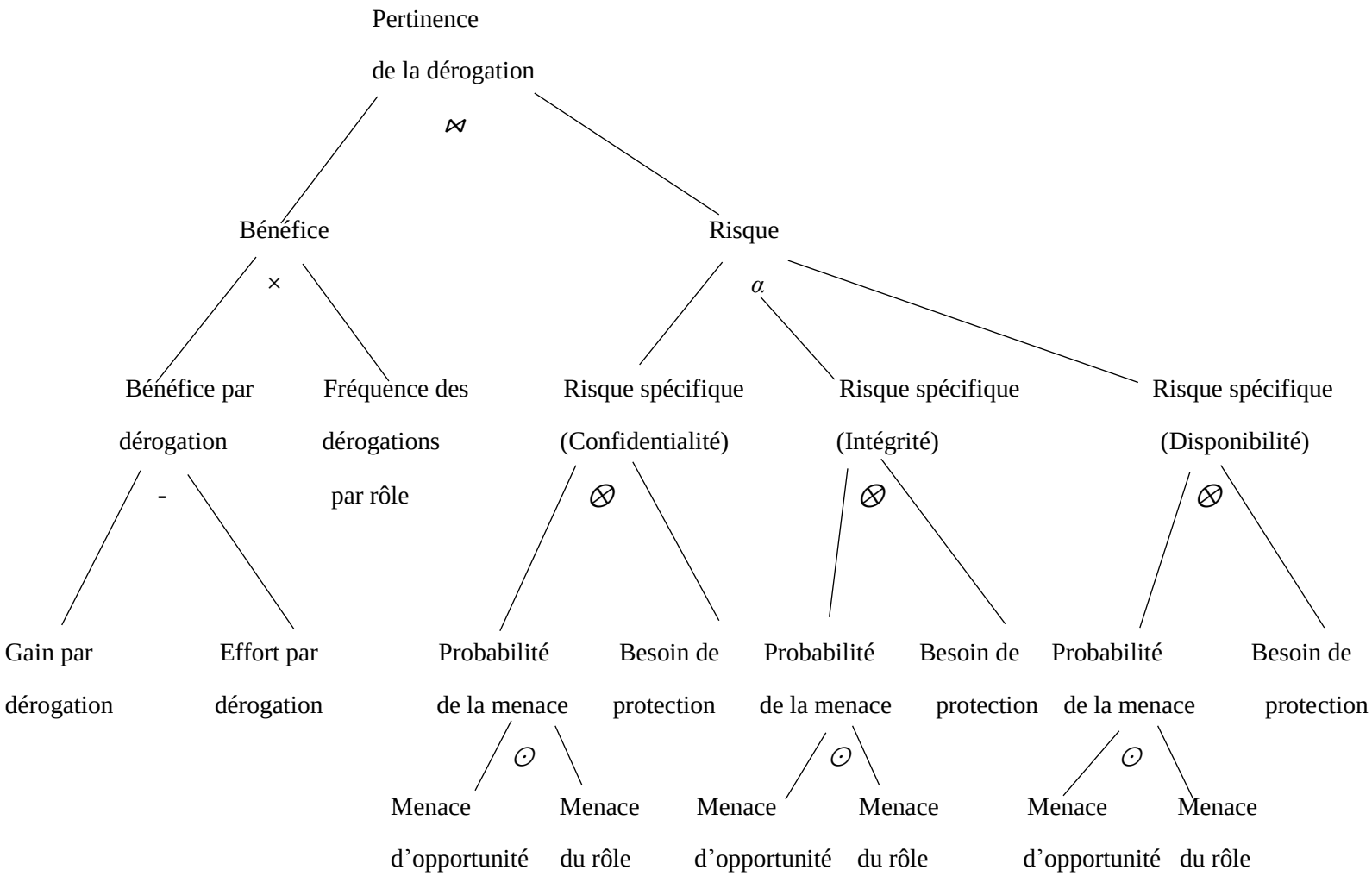


Figure 10. Récapitulation de la méthode

4.4.4 Discussion

Dans ce travail, *Bartsch* propose une méthode qui permet d'évaluer qualitativement le risque de dérogation aux politiques d'accès dans *RBAC*. En général, les méthodes qualitatives fournissent une voie plus facile pour mesurer la valeur du risque. Ces valeurs peuvent être décrites en utilisant des niveaux tels que "*très élevé*", "*élevé*" et "*faible*". Cela dit, une méthode quantitative pourrait être plus performante et plus précise puisqu'elle s'appuie sur des données chiffrées. Dans notre travail, nous présentons tant des méthodes qualitatives que des méthodes quantitatives.

4.5 RBAC basé sur le risque

Chen et al. [19] présentent trois modèles qui intègrent les concepts du risque dans le modèle *RBAC*. Ces modèles peuvent être combinés pour former un modèle général basé sur le risque. Ainsi, le risque d'accorder un accès dans le modèle *RBAC* peut être formulé en considérant la *fiabilité de l'utilisateur*, le *degré de compétence d'un utilisateur pour un rôle* et le *degré de pertinence d'une affectation permission-rôle*. Des composants logiciels appropriés sont supposés être en mesure d'évaluer ces facteurs et ajuster dynamiquement leurs valeurs lorsque le contexte est modifié.

Un formalisme à base de graphes définit la sémantique de ces modèles : *U*, *R* et *P* représentent respectivement les *utilisateurs*, les *rôles* et les *permissions*. *UA*, *PA* et *RH* représentent respectivement l'*affectation des utilisateurs aux rôles*, l'*affectation des permissions aux rôles* et la *hiérarchie des rôles*.

Un état de *RBAC (UA, PA, RH)* est représenté par un graphe acyclique orienté $G = (V, E)$. $V = U \cup R \cup P$ et $E = UA \cup PA \cup RH$. Chaque sommet $v \in V$ représente une entité : un utilisateur *u*, un rôle *r* ou une permission *p*. Chaque arête dirigée $e = (vi, vj)$ représente une relation entre deux entités v_i et vj. $(v_i, v_j) \in E$ si et seulement si l'une des conditions suivantes est vraie : $(v_i, v_j) \in UA$, $(v_j, v_i) \in RH$ ou $(v_j, v_i) \in PA$.

Un *trajet d'autorisation au-chemin* entre v_1 et v_n est une séquence de sommets $v_1, \ldots, v_n$ tel que $(v_i, v_{i+1}) \in E$ avec $i = 1, \ldots, n - 1$. Un utilisateur *u* peut activer un rôle *r* s'il existe

un *au-chemin* entre *u* et *r*. Un rôle *r* a la permission *p* s'il existe un *au-chemin* entre *r* et *p*. Un utilisateur *u* a la permission *p* s'il existe un *au-chemin* entre *u* et *p*. En d'autres termes, déterminer si un utilisateur *u* est autorisé à invoquer une permission revient à trouver un chemin comprenant un rôle actif de *u* à *p*.

4.5.1 Modèle RBAC$_T$

Le modèle *RBAC$_T$ Trustworthiness and role-based access control* enrichit le modèle standard *RBAC* avec deux fonctions $\alpha : U \rightarrow [0, 1]$ et $\lambda : P \rightarrow M$.

α(u) désigne le degré de fiabilité de l'utilisateur *u*, *M* désigne l'ensemble des stratégies d'atténuation des risques et *λ(p)* désigne la stratégie d'atténuation des risques associée à l'utilisation de la permission *p*. Pour calculer le risque d'accorder une permission *p* à un utilisateur *u*, une fonction de risque $Risk_T : U \times P \rightarrow [0, 1]$ est définie comme suit :

$$Risk_T(u, p) = \begin{cases} 1 - \alpha(u) \; s'il \; existe \; un \; au - chemin \; de \; u \text{ à } p \\ 1 \; sinon \end{cases}$$

S'il n'existe pas un *au-chemin* de *u* à *p*, $Risk_T(u, p)$ est égal à *1* et la demande d'accorder la permission *p* à l'utilisateur *u* sera refusée. S'il existe un *au-chemin* allant de *u* à *p*, le risque est déterminé en considérant la fiabilité de *u* déterminée par *α(u)*.

Exemple : soient deux demandes (u_1, p) et (u_2, p). $Risk_T(u_1, p) < Risk_T(u_2, p) < 1$ signifie que l'attribution de *p* à u_2 est plus risquée que l'attribution de la même permission *p* à u_1, puisque u_1 est plus fiable que u_2.

Une fonction de décision d'autorisation $Auth_T$ est définie comme suit : pour un état de $RBAC_T(V, E, \alpha, \lambda)$, une demande d'accès *(u, p)* et une stratégie d'atténuation du risque $\lambda(p) = [(0, \perp), (t_1, b_1), \ldots, (t_{n-1}, b_{n-1}), (t_n, \perp)]$ retournent une décision d'autorisation (permettre ou refuser) et une obligation *bi* qui dépend de la valeur du risque t_i où $1 \leq i < n$. Une *obligation* est un ensemble d'actions qui doivent être exécutés par le *point d'application de la politique* (*PEP*) suite à l'application d'une décision de contrôle d'accès. $\perp$ désigne l'obligation "null" c'est-à-dire aucune action ne doit être exécutée suite à une permission ou à un refus d'accès.

Exemple :

- *(0, ⊥)* signifie que pour une valeur de risque égale à *0* aucune action ne doit être exécutée lorsque l'accès est permis.
- *(t_1, b_1)* signifie que pour une valeur de risque égale à t_1 l'obligation *bi* doit être exécutée lorsque l'accès est permis.

Formellement, $Auth_T$ est définie comme suit :

$$Auth_T((V, E, \alpha, \lambda), (u, p), \lambda(p)) = \begin{cases} (permettre, \perp) \; si \; risk_T(u,p) < t_1, \\ (permettre, b_i) \; si \; risk_T(u,p) \in [t_i, t_{i+1}], \\ (refuser, \perp) \; si \; risk_T(u,p) \geq t_n. \end{cases}$$

En d'autres termes, la demande de *u* pour exécuter *p*, est autorisée s'il existe un *au-chemin* de *u* à *p* dans le graphe $RBAC_T$ et $Risk_T(u, p)$ est inférieur à un seuil de risque t_1 spécifié pour la permission *p*. Lorsque le risque est relativement élevé (dans un intervalle $[t_i, t_{i+1}]$ où $1 \leq i < n$), la permission d'accès implique l'exécution d'un ensemble d'obligations b_i. Lorsque le risque est très élevé $(Risk_T(u, p) \geq t_n)$ l'accès est refusé.

4.5.2 Modèle $RBAC_C$

Le modèle $RBAC_C$ enrichit le modèle standard de *RBAC* avec deux fonctions $\beta : U \times R \rightarrow [0, 1]$ et $\lambda : P \rightarrow M$.

$\beta(u, r)$ désigne le degré de compétence d'un utilisateur *u* pour effectuer un rôle *r*, et $\lambda(p)$ désigne la stratégie d'atténuation des risques associée à l'utilisation de *p*. Pour tout $(u, r) \in UA$, $\beta(u, r) > 0$. En effet, il n'est pas utile d'affecter *u* à *r* si *u* n'est pas compétent pour exercer le rôle *r*. À la différence de $RBAC_T$, $RBAC_C$ définit la notion de *compétence* pour les affectations *utilisateur-rôle*, ce qui conduit à une façon différente de calculer le risque des demandes d'accès.

Soit l'état de $RBAC_C$ $G = (V, E, \beta, \lambda)$. $(v, *)$ désigne l'ensemble des entités qui sont connectées à *v* par des arêtes. $(v, *) = \{v' \in V: (v, v') \in E\}$. $(*, v)$ désigne l'ensemble des entités qui sont connectés à *v*. Formellement, $(*, v) = \{v' \in V: (v', v) \in E\}$. Par souci de concision, on écrit $v *$ pour $(v, *)$ et $* v$ pour $(*, v)$.

Pour tout $v \in V$, $\downarrow v$ désigne l'ensemble des entités pour lesquelles v est autorisé dans *RBAC*. $\downarrow v = \{v' \in V$: *il existe un au-chemin de v à v'}*. De même $\uparrow v = \{v' \in V$: *il existe un au-chemin de v' à v}*.

Pour une demande *(u, p)*, il peut y avoir plusieurs chemins entre *u* et *p* dans le graphe de $RBAC_C$. L'ensemble des rôles pour lesquels *u* est explicitement autorisé et qui se trouvent sur un *au-chemin* de *u* à *p*, est $u^* \cap \uparrow p$. C'est-à-dire l'ensemble des nœuds qui représentent des rôles dans le graphe et qui se trouvent sur un *au-chemin* entre le nœud qui représente l'utilisateur et le nœud qui représente la permission.

Pour calculer le risque de *(u, p)*, le niveau de compétence de *u* pour effectuer chaque rôle dans $u^* \cap \uparrow p$, est pris en considération. Pour une demande *(u, p)*, il peut exister un ou plusieurs *au-chemins* de *u* à *p*. C'est à dire, *u* est compétent pour effectuer tous les rôles dans $u^* \cap \uparrow p$. Le risque de *(u, p)* est déterminé en trouvant un *au-chemin u, r, . . ., p* tel que $\beta(u, r)$ est maximale.

Le rôle pour lequel *u* est plus compétent, est considéré lors de l'évaluation de la demande d'accès. Formellement, $Risk_C : U \times P \rightarrow [0, 1]$ est définie comme suit :

$$Risk_C(u, p) = \begin{cases} 1 \text{ si } u^* \cap \uparrow p = \emptyset, \\ 1 - max\{\beta(u, r) : r \in u^* \cap \uparrow p\} \text{ autrement.} \end{cases}$$

Exemple : considérons le graphe orienté d'une configuration de $RBAC_C$ représenté par la *Figure 11* [19], avec $\beta(u_1, r_1) = \beta(u_2, r_3) = 1/2$ et $\beta(u_1, r_2) = \beta(u_2, r_2) = 1/3$. u_1 est en mesure d'exécuter p_1 à travers le rôle r_1 pour lequel u_1 est le plus compétent. Ainsi, $Risk_C(u_1, p_1) = 1 - 1/2 = 1/2$. Cependant, $Risk_C(u_1, p_3) = 1$ puisque $u^* \cap \uparrow p_3 = \{r_1, r_2\} \cap \{r_3\} = \emptyset$ ce qui signifie qu'il n'y a pas un *au-chemin* de u_1 à p_3.

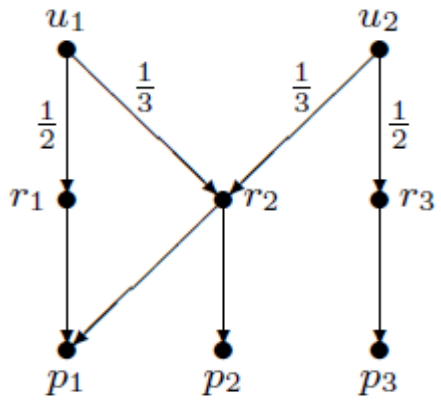


Figure 11. Représentation graphique de l'état de $RBAC_C$ [19]

La fonction de décision d'autorisation $Auth_C$ (similaire à $Auth_T$) est définie comme suit :

$$Auth_C((V, E, \beta, \lambda), (u, p), \lambda(p)) = \begin{cases} (permettre, \perp) si\ risk_C(u,p) < t_1, \\ (permettre, b_i) si\ risk_C(u,p) \in [t_i, t_{i+1}], \\ (refuser, \perp)\ si\ risk_C(u,p) \geq t_n. \end{cases}$$

4.5.3 Modèle $RBAC_A$

Le modèle *$RBAC_A$ Appropriateness and role-based access control* enrichit le modèle standard *RBAC* avec deux fonctions $\gamma : P \times R \rightarrow [0, 1]$ et $\lambda : P \rightarrow M$.

$\gamma (p, r)$ désigne le *niveau de la pertinence de l'affectation de la permission p au rôle r* et $\lambda (p)$ désigne la stratégie d'atténuation des risques associés à l'utilisation de *p*. Pour tout $(p, r) \in PA$, $\gamma(p, r) = 0$.

$RBAC_A$ introduit une approche de calcul du risque similaire à *$RBAC_C$* et *$RBAC_T$*. Ce modèle ajoute le concept de *pertinence des affectations permission-rôle*.

* *p* désigne l'ensemble des rôles auxquels *p* est explicitement attribuée. * $p \cap \downarrow u$ désigne l'ensemble des rôles dans * *p* auxquels *u* est attribué. En d'autres termes, * $p \cap \downarrow u$ est l'ensemble de rôles auxquels *p* est explicitement affecté et qui se trouvent sur un *au-chemin* entre *u* et *p*.

$p \in P$ peut être explicitement affectée à plusieurs rôles. Un niveau de pertinence est associé à chaque affectation. Un utilisateur *u* peut exécuter *p* en activant le rôle le plus

pertinent auquel *p* est affecté. Ce rôle sera considéré pour l'évaluation du risque de la demande d'accès.

La fonction de risque $RISK_A : U \times P \rightarrow [0, 1]$ est définie comme suit :

$$RISK_A(u, p) = \begin{cases} 1 \; si \; * p \cap \downarrow u = \emptyset, \\ 1 - max\{\gamma(p, r) : r \in * p \cap \downarrow u\} \; autrement \end{cases}$$

Prenons l'exemple de l'état de $RBAC_A$ dans la *Figure 12* [19], u_2 est capable d'exécuter p_1 par l'intermédiaire de r_1 ou r_2. Cependant, le rôle r_1 est le plus approprié pour p_1. Ainsi, la valeur de γ qui est *1/2* pourrait être considérée. $RISK_A(u_2, p_1) = 1/2$.

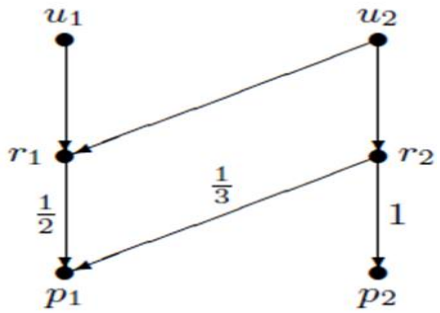


Figure 12. Représentation graphique de l'état de $RBAC_A$ [19]

Soient l'état $RBAC_A(V, E, \gamma, \lambda)$, une demande d'accès (u, p) et une stratégie d'atténuation des risques $\lambda(p)$ pour la permission *p*. La fonction de décision d'autorisation $Auth_A$ (similaire à $Auth_T$ et $Auth_C$) est définie comme suit :

$$Auth_A((V, E, \gamma, \lambda), (u, p), \lambda(p)) = \begin{cases} (permettre, \perp) \; si \; risk_A(u, p) < t_1, \\ (permettre, b_i) \; si \; risk_A(u, p) \in [t_i, t_{i+1}], \\ (permettre, \perp) \; si \; risk_A(u, p) \geq t_n. \end{cases}$$

4.5.4 Modèle général

Un modèle R^2BAC basé sur le risque peut combiner les caractéristiques des modèles $RBAC_T$, $RBAC_C$ et $RBAC_A$. Ainsi, le risque associé à un *au-chemin u, r,. . . , r', p*, peut être calculé comme suit :

$$1 - min\{\alpha(u), \beta(u, r), \gamma(r', p)\}$$

En d'autres termes, le risque associé au *au-chemin u, r,. . ., r', p* est déterminé par la valeur minimale de l'ensemble comprenant la fiabilité de *u*, le niveau de compétence de *u* pour exercerle rôle *r* et le niveau de pertinence de l'affectation de *p* à *r'*.

Le risque associé à un*au-chemin* peut être calculé comme suit aussi :

$$min \{1, (1 - \alpha (u)) + (1 - \beta (u, r)) + (1 - \gamma (r', p))\}.$$

Ce calcul accumule les risques associés à chaque partie du chemin.

4.5.5 Discussion

Ce travail fournit un ensemble de concepts élégants pour la modélisation du risque dans *RBAC*. En effet, il présente trois modèles qui intègrent les concepts du risque dans ce modèle. Ces modèles peuvent être combinés pour former un modèle général. Cependant ce modèle général ne montre pas comment quantifier la fonction β qui désigne le degré de compétence d'un utilisateur *u* pour effectuer un rôle *r*, et la fonction γ qui désigne le niveau de la pertinence de l'affectation de *p* à *r*. Ce travail ne montre pas aussi comment les stratégies d'atténuation des risques sont associées aux permissions et comment elles peuvent changer selon le contexte. Notre travail vise à amorcer une solution à ce problème et des recherches futures pourraient montrer l'applicabilité de nos résultats dans le contexte des modèles que nous avons présentés.

4.6 Modèle basé sur le risque et utilisant la logique floue

Dans ce travail, *Cheng et al*. [20] présentent le modèle *MLS flou* utilisé pour gérer les accès aux informations du *Système S* d'*IBM* [52], un système conçu pour analyser une grande quantité de données par des analystes financiers. Ce système doit assurer l'analyse, la protection, et la disponibilité de ses informations tout en gérant le risque de divulgation d'informations sensibles.

4.6.1 Calcul du risque : système multi-niveaux flou

Contrairement aux modèles *MLS traditionnels* qui donnent des décisions d'accès binaires (Acceptation ou refus), le modèle *MLS flou* permet d'accepter des accès qui seraient refusés par les modèles d'accès traditionnels mais il exige la mise en place des mesures de mitigation du risque.

L'approche présentée dans ce travail définit deux limites :

- Une *limite dure* (*Hard boundary*) : les demandes d'accès qui ont une valeur de risque au-dessus de cette limite sont considérées très risquées et sont refusées par défaut.
- Une *limite douce* (*Soft boundary*) : les demandes d'accès qui ont une valeur de risque au-dessous de cette limite ne représentent pas de risque et sont acceptées par défaut.

Pour les accès acceptés ayant des valeurs de risque entre la limite douce et la limite dure, des mesures de mitigation du risque sont mises en place. Ces mesures sont déterminées selon la bande du risque dans laquelle la valeur calculée est située comme nous pouvons le voir dans la *Figure 13*.

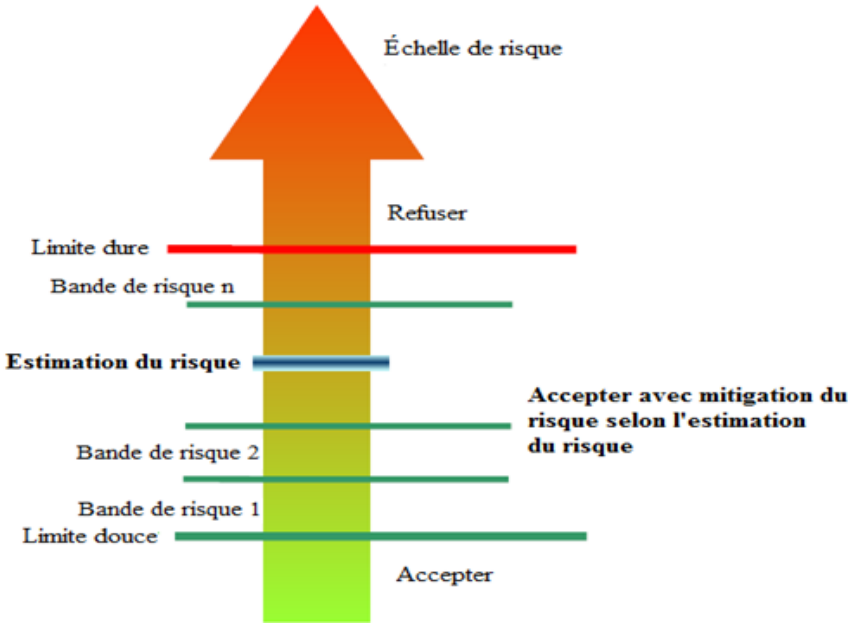


Figure 13. Une échelle de risque (adaptée de [20])

MLS Flou étend le modèle de sécurité *multi-niveaux Bell-LaPadula (BLP)* pour qu'il soit basé sur la *gestion des risques*. Pour un utilisateur humain, le risque d'un accès en lecture est défini par la formule suivante :

$$Risque = (probabilité\ du\ préjudice) \times (valeur\ de\ l'information)$$

La « *valeur* » de l'information est définie comme le préjudice subi si cette information accédée est divulguée d'une façon non autorisée. Pour estimer la valeur des informations, les organisations leur attribuent des niveaux de sensibilité.

Déterminer de façon précise la *probabilité* de divulgation non autorisée, est généralement impossible, car cela nécessite la prévision du comportement futur des utilisateurs. Le modèle proposé présente une méthode qui permet d'attribuer ces probabilités en se basant sur les idées intuitives suivantes :

La *probabilité* devrait être très élevée dans le cas d'une personne sans habilitation de sécurité qui a accès à des informations secrètes mais relativement faible si l'accès est accordé à une personne qui a un niveau d'habilitation très élevée.

D'après ces principes, la probabilité *P* dans le modèle *Bell-LaPadula traditionnel* peut être estimée à partir de deux probabilités indépendantes *P1* et *P2* [20] :

$$P = P1 + P2 - P1 \times P2$$

$$P1 = \begin{cases} 0\ si\ \ le\ \ niveau\ d'habilitation\ du\ sujet\ \geq\ niveau\ de\ sensibilité\ de\ l'objet \\ 1\ sinon \end{cases}$$

$$P2 = \begin{cases} 0\ si\ la\ catégorie\ de\ l'utilisateur\ humain\ \supseteq\ catégorie\ de\ l'objet \\ 1\ sinon \end{cases}$$

P1 peut être vue comme la probabilité de la tentation d'un sujet humain (un utilisateur). *P2* peut être vue comme la probabilité de la divulgation de l'information par inadvertance. Ce travail présente une méthode qui donne une estimation non binaire de *P1* et *P2* contrairement au modèle *Bell-LaPadula* traditionnel. Ainsi, le modèle *MLS Flou* permet de quantifier le risque pour les accès qui violent la propriété simple du modèle *Bell-LaPadula*.

4.6.1.1 Calcul de P1

Le calcul de P1 se base sur l'idée suivante :

La tentation d'un sujet humain est fonction de son niveau d'habilitation (*sl*) qui représente son niveau de fiabilité et le niveau de sensibilité de l'objet (*ol*) qui représente la valeur de l'objet. Cette tentation devrait augmenter monotonement par rapport à *ol* et diminuer monotonement par rapport à *sl*.

BLP traditionnel a une vision binaire de la tentation dans le cas des accès en lecture : aucune tentation si $ol \leq sl$ et une tentation complète autrement. *BLP* utilise également une fonction pour relier la tentation à la probabilité de divulgation *P1* : aucune divulgation s'il n'y a pas de tentation et une divulgation avec une probabilité de *1* s'il y a tentation.

4.6.1.2 Calcul de P2

Le calcul de *P2* est basé sur les idées suivantes :

Quand un sujet humain a un fort besoin légitime d'accéder aux informations d'une catégorie, l'organisation est plus disposée à accepter la probabilité de divulgation par *inadvertance*. Par contre lorsqu' un sujet humain n'a pas un fort besoin d'accéder à des informations, l'organisation est moins disposée à accepter la probabilité de divulgation par inadvertance.

Si un sujet accède à un objet appartenant à une seule catégorie, *P2* est la différence entre la probabilité de divulgation par inadvertance et la probabilité que l'organisation est prête à accepter. *P2* est égale à zéro si la différence est négative. Si l'objet appartient à plusieurs catégories, la différence est calculée pour chaque catégorie. *P2* est égale à la valeur maximale des valeurs calculées pour chaque catégorie. Une valeur dans l'intervalle *[0, 1]* est attribuée à chaque sujet. Cette valeur représente son appartenance floue à une catégorie *c* et quantifie la nécessité de l'accès du sujet à l'information de cette même catégorie. Une valeur dans l'intervalle *[0, 1]* est attribuée à chaque objet. Cette valeur représente son appartenance floue à une catégorie *c* et quantifie la pertinence de l'appartenance de cet objet à cette même catégorie. Ainsi, *P2* diminue quand l'appartenance d'un sujet diminue et l'appartenance d'un objet augmente.

4.6.2 MLS flou dans le système S

Dans le cas d'une organisation qui exécute une instance du système S, le risque quantifié peut être considéré comme un montant limité. Ce montant représente la tolérance au risque de l'organisation. Le système *S* met en œuvre *MLS flou* de la manière suivante :

1. L'organisation détermine le montant maximum du risque de divulgation d'informations ORG_{CAP}.
2. ORG_{CAP} est réparti entre les employés de l'organisation qui utilisent le système *S*. La part d'un employé de ORG_{CAP} est U_{CAP}.
3. Un utilisateur *U* soumet une demande d'accès et indique le montant maximal de risque I_{CAP} qu'il est prêt à dépenser pour un accès donné. I_{CAP} doit être inférieur ou égal à *UCAP*.
4. Le système prend en considération I_{CAP} pour générer des plans qui pourraient satisfaire les requêtes. Chaque plan *P* est associé à une valeur de risque *Prisk* qui est calculée en utilisant *MLS Flou*et le contenu du plan. Le *planificateur* s'assure que *Prisk* est inférieur ou égale à I_{CAP}.
5. L'utilisateur *U* choisit un plan parmi les plans qui lui sont présentés.
6. Si le plan choisi est instancié, son *Prisk* est déduit de U_{CAP}. Ainsi, la nouvelle valeur de U_{CAP} limite la quantité du risque que *U* peut prendre.

4.6.3 Discussion

Le modèle *MLS flou* présentée, dans cette section, permet d'accepter des accès qui seraient refusés par *BLP* traditionnel mais il exige la mise en place des mesures de mitigation du risque. Cependant, cette approche :

- ne permet pas l'évaluation du risque dans les systèmes de contrôle d'accès pour les accès en écriture,
- ne permet pas de calculer le risque des accès lorsque l'objectif d'intégrité est visé,
- ne permet pas de prendre en considération de facteurs tels que les mesures d'atténuation des risques mises en place, la sécurité des environnements physiques

et logiques, l'historique des accès, les propriétés des canaux d'information qui peuvent affecter les estimations du risque,

- est basée sur l'idée que les étiquettes de sécurité sont exactes et correctes. En réalité, l'exactitude de l'affectation de ces étiquettes n'est pas évidente. Exprimer explicitement l'incertitude dans les affectations des étiquettes par des fonctions mathématiques peut améliorer la qualité des décisions d'accès dans les systèmes *MLS* puisque ces décisions se basent sur les niveaux de sensibilité des objets et les niveaux d'habilitation des sujets.

L'approche que nous proposons dans le cadre de notre travail, cherche à aller plus loin dans chacune de ces directions. En effet, notre approche permettrait d'évaluer le risque des accès en écriture et le risque des accès lorsque l'objectif d'intégrité est visé, de prendre en considération des facteurs tels que les mesures d'atténuation des risques mises en place, et de considérer l'historique des accès pour déterminer les niveaux de sensibilité des objets et les niveaux d'habilitation des sujets. La prise en compte de ces facteurs pourrait se traduire par un modèle plus réaliste pour les environnements dynamiques.

4.7 Modèle pour la protection de renseignements personnels dans les systèmes de santé

Wang et al. [96] proposent un modèle de contrôle d'accès pour la protection des renseignements personnels des patients dans les systèmes d'informations de santé. Ce modèle permet :

- de déterminer des décisions d'accès aux données médicales en se basant sur la quantification du risque,
- d'observer les pratiques courantes chez les médecins et appliquer des méthodes statistiques et des techniques de la théorie de l'information pour quantifier le risque de violation de la confidentialité,
- de prendre en compte les besoins d'accès exceptionnels.

4.7.1 Méthode de calcul du risque

La méthode proposée de calcul des valeurs de risque suit les étapes suivantes :

1. Lorsqu'un médecin demande d'accéder à un dossier médical, son accès est marqué avec une *finalité* (*purpose*).
2. Le système de contrôle d'accès tient un journal de tous les accès des médecins et enregistre la finalité de chaque accès et l'étiquette du document demandé.
3. Des scores de risque sont calculés périodiquement. Le degré de risque dépend de la pertinence, par rapport à la finalité, des accès d'un médecin aux documents consultés dans la dernière période.
4. Des scores de risque d'un médecin dans des périodes de temps différentes sont agrégés et utilisés pour déterminer ses accès.

Dans ce qui suit, nous décrivons les trois étapes importantes dans cette méthode de quantification des risques.

4.7.1.1 Étiquetage des dossiers médicaux et des demandes d'accès

La plupart des hôpitaux classent les dossiers de leurs patients en utilisant des codes de diagnostic, tels que *ICD-9*. Les codes de diagnostic peuvent être utilisés comme les étiquettes des dossiers médicaux. Ainsi, les demandes d'accès peuvent également être marquées avec des codes de diagnostic.

4.7.1.2 Estimation de la pertinence des documents médicaux pour une finalité

Une étape importante dans cette méthode de quantification du risque consiste à déterminer comment différents types de dossiers sont liés à des finalités diverses. D'où la nécessité d'estimer le degré de pertinence d'un dossier médical pour une finalité. On suppose que généralement, les connaissances professionnelles des médecins leur permettent de sélectionner correctement l'information qui est utile pour leurs tâches. Étant donné une finalité t_i, l'observation de la distribution des étiquettes de documents médicaux demandés par les médecins pour t_i, permet d'avoir des connaissances sur la façon avec laquelle différents types de documents sont utiles pour t_i.

4.7.1.3 Calcul des valeurs du risque

Un médecin peut avoir besoin d'un document pour servir une finalité. Au lieu de mesurer le risque de chaque accès, les auteurs proposent de traiter l'ensemble des demandes faites par un médecin pour la même finalité pendant une période de temps, et calculer une valeur de risque pour un tel ensemble de demandes. La valeur du risque dépend de la façon dont la combinaison de documents demandés sert la finalité du médecin. À noter que le médecin peut servir plusieurs patients pour la même finalité.

L'approche proposée consiste à comparer la combinaison des étiquettes des dossiers accédés par un médecin avec ceux accédés par tous les médecins. Pour quantifier le résultat de la comparaison, le concept de *l'entropie de Shannon* est utilisé. L'*entropie* est une mesure de l'incertitude associée à une variable aléatoire. Soit T_i l'ensemble des finalités figurant dans les demandes d'accès du médecin u_i pendant la dernière période. Pour chaque finalité $t_j \in T_i$, $S(u_i, t_j)$ est la séquence des étiquettes des dossiers demandés par u_i pour la réalisation de la finalité t_j dans la dernière période. Soit $f_{ui}(l_k, t_j)$ le nombre d'occurrences de dossiers médicaux avec l'étiquette $l_k \in L$ dans $S(u_i, t_j)$.

La probabilité qu'un dossier médical avec l'étiquette l_k soit choisi par u_i pour la finalité t_j est donnée par la formule suivante :

$$p_{ui}(l_k \mid t_j) = f_{ui}(l_k, t_j) / \sum_{l_b \in L} f_{ui}(l_b, t_j)$$

Soit x la variable aléatoire correspondant à la sélection des dossiers médicaux. L'incertitude des dossiers médicaux sélectionnés par u_i pour la finalité t_j peut être calculée par la formule suivante :

$$H_{ui}(t_j, x) = -\sum_{k=1}^{|L|} p_{ui}(l_k \mid t_j) \ln p_{ui}(l_k \mid t_j)$$

De même, la méthode consiste à calculer $H_{all}(t_j, x)$ qui représente l'incertitude sur la sélection des dossiers médicaux de tous les médecins pour la finalité t_j. Le risque associé aux demandes de u_i pour la finalité t_j dans la dernière période est représenté par la différence entre les deux incertitudes ci dessus et peut être calculé comme suit :

$$R(u_i, t_j) = \max\{H_{ui}(t_j, x) - H_{all}(t_j, x), 0\}$$

La valeur de $R(u_i, t_j)$ est non-négative.

Les étiquettes des dossiers médicaux des médecins malveillants seraient plus diversifiées que celles des accès de tous les médecins ce qui conduit à une incertitude plus élevée et donc une plus grande *entropie*. Cela donne un niveau de risque plus élevé.

4.7.1.4 Contrôle d'accès basé sur le risque

Les valeurs de risque sont calculées périodiquement pour chaque médecin. Au début, un quota d'accès est attribué à chaque médecin. Chaque fois qu'une valeur de risque est calculée pour un médecin, le quota d'accès est déduit de son compte. Le médecin peut continuer à accéder aux dossiers médicaux tant que la valeur de ses quotas restants est supérieure à zéro. Autrement dit, ses autres demandes d'accès seront refusées jusqu'à ce qu'il acquière plus de quotas.

Un certain nombre de nouveaux quotas sont prévus périodiquement pour chaque médecin. Le nombre de quotas alloués est supposé être suffisant pour les demandes d'accès du médecin au cours d'une période de temps déterminée. Ce nombre de quotas accordés à un médecin spécifie essentiellement un niveau de risque que le système peut tolérer pour un médecin pendant une période de temps.

4.7.2 Discussion

Le travail présenté, dans cette section, consiste à appliquer des méthodes statistiques et des techniques de la théorie de l'information pour quantifier le risque d'accès aux données médicales. L'intuition derrière le calcul du risque, est qu'un choix plus diversifié des dossiers médicaux conduit à une incertitude plus élevée et donc une plus grande entropie, ce qui conduit à un niveau de risque plus élevé. Cette hypothèse n'est pas valable dans toutes les circonstances, étant donné que plusieurs médecins peuvent avoir besoin d'accéder à des dossiers diversifiés dans le cadre de leurs tâches routinières.

4.8 Systèmes de contrôle d'accès basés sur le risque établi sur des inférences floues

Ce travail [77] propose un *système d'inférence floue* (*Fuzzy inference system*) pour les systèmes de contrôle d'accès basés sur les risques. Ce système propose une approche

mathématique qui permet de déduire une conséquence non ambiguë à partirde preuves vagues et de règles *si-alors*subjectives. Les facteurs de risques utilisés parcette approche sont les niveaux de sécurité des sujets et des objets.

4.8.1 Bell-LaPadula flou

Considérons un système qui permet de calculer le score de sensibilité d'un document en considérant quatre catégories qui ont des limites supérieures : les auteurs (*300*), le contenu (*300*), les départements (*200*) et le public destiné (*200*). Chaque catégorie a des propriétés facultatives et d'autres obligatoires ayant des valeurs différentes. Chaque valeur a un score de sensibilité défini par des experts de sécurité. Le score d'un document est égal à la somme des scores des propriétés. Le plus bas score d'un document (somme des scores les plus faibles des valeurs des propriétés obligatoires) est *500* et le score le plus élevé est *1000*.

Les niveaux de sécurité des documents sont *Unclassified*, *Classified*, *Secret* et *Top secret*. Les scores des niveaux de sécurité *x* sont comme suit : *500-600* (*Unclassified*), *601-750* (*Classified*), *751-900* (*Secret*) et *901-1000* (*Top secret*).

La sensibilité d'un document avec un score *x* de *601* (*Classified*) peut être surestimée alors que la sensibilité d'un document avec un score *x* de 600 (*Unclassified)* peut être sous-estimée. Pour faciliter la transition entre les niveaux de sécurité, les auteurs proposent d'appliquer la fonction suivante :

$$trapmf\ (x, a, b, c, d) = max\ (min\ (\frac{x-a}{b-a}\ ,1,\frac{x-a}{b-a}),0)$$

Une fonction d'appartenance est définie pour chaque niveau de sécurité :

- *Unclassified: uc(x) = trapmf (x; 500, 500, 550, 650).*
- *Classified: c(x) = trapmf (x; 550, 650, 700, 800).*
- *Secret: s(x) = trapmf (x; 700, 800, 850, 950).*
- *Top Secret: ts(x) = trapmf (x; 850, 950, 1000, 1000).*

Le *degré d'appartenance* à un niveau de sécurité spécifique est déterminé par sa fonction d'appartenance. Par exemple, les degrés d'appartenance d'un document avec un score *x* de *600* sont les suivants : *0,5* (*Unclassified*), *0,5* (*Classified*), *0* (*Secret*), et *0* (*Top secret*). De

même, les degrés d'appartenance d'un document avec un score de *601* sont : *0,49* (*Unclassified*), *0,51* (*Classified*), *0* (*Secret*) et *0* (*Top secret*).

Les auteurs considèrent aussi :

- un système de score d'habilitation des sujets et une fonction d'appartenance pour chaque niveau de sécurité,
- un système de score du risque et cinq fonctions d'appartenance pour les estimations du risque : *très faible* (*extremely low*), *faible* (*low*), *moyen* (*medium*), *élevé* (*high*) et *très élevé* (*extremely high*).

Le *Tableau 7* représente des règles "*si antécédents alors conséquences*" (*if antecedent then consequent*) pour mettre en œuvre un système *BLP* basé sur le risque. Ces règles déterminent un risque d'accès en considérant la classification de l'objet et le niveau de sécurité du sujet.

Exemple : la règle *1* stipule que si le niveau de sécurité de l'objet est *non classé* (*Unclassified*), le risque d'accès est extrêmement *faible* (*extremely low*). De même, la règle *2*stipule que si le niveau de sécurité du sujet n'est pas *non classé* (*not unclassified*) et le niveau de sécurité de l'objet est *classé* (*Classified*), alors le risque d'accès est faible (*low*). La dernière colonne du *Tableau 7* représente le poids des règles.

	Antecedent		Consequent	
ID	Subject Label	Object Label	Risk	W
1	N/A	unclassified	extremely low	1.0
2	not unclassified	classified	low	1.0
3	unclassified	classified	medium	1.0
4	unclassified	secret	high	1.0
5	classified	secret	high	1.0
6	secret	secret	low	1.0
7	top secret	secret	low	1.0
8	not top secret	top secret	extremely high	1.0
9	top secret	top secret	medium	1.0

Tableau 7. Règles d'inférence du risque dans BLP [77]

4.8.2 Exemple d'application

La procédure pour évaluer le risque d'un accès d'un sujet avec un score de *750* à un document avec un score de *750* est comme suit :

4.8.2.1 Calcul des degrés d'appartenance (Fuzzification)

Cette étape consiste à calculer les degrés d'appartenance du sujet et de l'objet à chaque niveau de sécurité selon leurs fonctions d'appartenance prédéfinies. Soient les degrés d'appartenance du sujet : *0,0076* (*non classé*), *0,5814* (*classé*), *0,5814* (*secret*), et *0,0076* (*top secret*). Soient les degrés d'appartenance du document : *0* (*non classés*), *0,5* (*classé*), *0,5* (s*ecret*), et *0* (*top secret*).

4.8.2.2 Application des opérations floues

Cette étape consiste à calculer le degré de confiance d'une règle en se basant sur les degrés d'appartenance et les conditions logiques (*Si-alors*) dans l'antécédent de la règle.

Le degré de confiance d'une règle est obtenu par la fonction suivante où *x* représente le degré d'appartenance du sujet et *y* le degré d'appartenance de l'objet : $Tp(x, y) = x \times y$. Par exemple, le degré de confiance de la règle *5* est $0,5814 \times 0,5 = 0,2907$.

4.8.2.3 Application de la méthode d'implication

Cette étape consiste à calculer l'estimation du risque d'une règle basée sur la conjonction de sa conséquence, son poids et le degré d'appartenance de la conséquence. Par exemple, l'estimation du risque de la règle 5 est : $0,2907 \times mfhigh \times 1$, avec *mfhigh* est la fonction d'appartenance de : *access risk is high* (*le risque d'accès est élevé*).

4.8.2.4 Agrégation de toutes les sorties

Cette étape consiste à calculer la valeur du risque à partir des estimations du risque de toutes les règles impliquées. Cette valeur est le résultat d'une fonction d'agrégation *rf*.

4.8.2.5 Génération du score final du risque (Defuzzification)

Cette étape génère le score final du risque en utilisant la fonction *rf* comme suit :

$$Risk = centroid\ (rf\ (x)) = \frac{\int rf(x)xdx}{\int rf(x)dx}$$

L'estimation finale du risque d'accès de notre exemple est égale à *38.6412*.

4.8.3 Contrôle du dommage

Cette section décrit la méthode présentée pour limiter les dégâts causés par des utilisateurs malicieux.

4.8.3.1 Quota d'accès

La solution présente le concept du *quota d'accès*. Un quota d'accès est un nombre de jetons d'accès. Il existe deux types de quotas d'accès : un quota d'accès pour les utilisateurs et un quota d'accès pour les obligations. L'idée de la solution pour contrôler les dommages est représentée par la *Figure 14* qui montre ce qui suit :

- Tous les *jetons d'accès* courants de sujets sont enregistrés dans une *table de suivi des jetons d'accès*.
- Lorsqu'un sujet demande l'accès à un objet, le nombre de ses jetons disponibles est vérifié après l'estimation du risque. Si le nombre de jetons d'accès disponibles est inférieur à la somme des quotas des obligations requises par l'accès, l'accès sera refusé.
- Si une demande d'accès est autorisée, la *table de suivi* est mise à jour en déduisant la somme des quotas des obligations requises par l'accès, des jetons d'accès du sujet.
- Lorsqu'une obligation a été respectée, la table de suivi est mise à jour en ajoutant les jetons d'accès du sujet déduits par l'obligation.

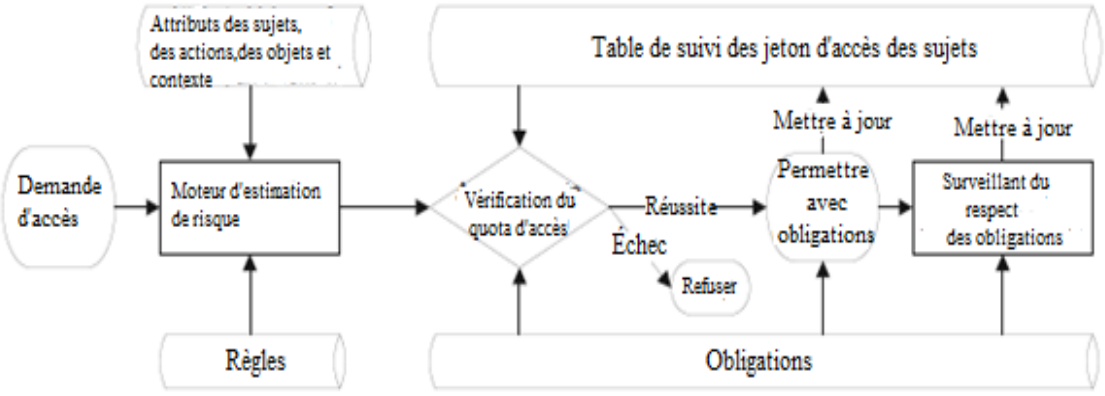


Figure 14. Méthode générale pour contrôler l'ensemble des dommages (adaptée de [77])

4.8.4 Solution basée sur l'inférence floue

Pour déterminer les cas où les règles d'inférence floue sont applicables, les auteurs introduisent une nouvelle fonction *Token Check* définie comme suit :

$$TokenCheck\ (s) = \begin{cases} 0\ if t(s) \leq \delta \\ 1\ if t(s) > \delta \end{cases}$$

s est un sujet, *t(s)* retourne le nombre courant de jetons du sujet *s* et δ est un seuil prédéfini pour un nombre minimum requis de jetons. Une *conjonction logique* lie chaque règle d'inférence floue à la fonction d'appartenance *TokenCheck(s)*. Ainsi, cette étape permet de s'assurer que, lorsque le nombre courant de jetons du sujet est en dessous du seuil δ, aucune des règles d'inférence floue ne sera applicable et un refus par défaut sera retourné.

4.8.5 Discussion

Il existe plusieurs applications réussies d'inférence floue dans les domaines de l'ingénierie, le système de navettes spatiales ou les systèmes de mise au point automatique d'appareils photo numériques. Des dizaines de paramètres et des centaines de règles d'inférence sont généralement suffisantes pour ces applications. Par conséquent, le temps de calcul est très faible. Cela n'est pas nécessairement vrai dans le cas des systèmes de contrôle d'accès qui fournissent des services pour des dizaines, des centaines ou des milliers d'utilisateurs simultanément.

4.9 Autres travaux

Dans cette section, nous présentons brièvement d'autres travaux connexes sur lesquels nous n'attardons pas en raison des contraintes d'espace.

Agrawal [2] présente un système de contrôle d'accès *risque-bénéfice* qui détermine les décisions d'accès en considérant plusieurs facteurs à savoir l'avantage personnel, les bénéfices organisationnels, les dommage organisationnels, le coût personnel, etc.

Zhang et al. [104] proposent un système de contrôle d'accès *risque-bénéfice*. Les valeurs du bénéfice et du risque sont des vecteurs multidimensionnels représentant des attributs

tels que la monnaie, la propriété intellectuelle, la propriété physique et la vie humaine. Les transactions sont autorisées lorsque le bénéfice global est supérieur au risque global pour chaque composante du vecteur.

Chari et al. [18] présentent un système d'évaluation du risque basé sur la logique floue. Les principales fonctions présentées dans ce travail sont :

- L'agrégation qui permet de calculer la sensibilité agrégée d'un groupe de permissions en considérant les niveaux de sensibilité des permissions considérées séparément ou le niveau de risque d'accès global de l'utilisateur.
- L'inférence qui permet de déduire le risque de l'attribution d'un rôle (un ensemble de permissions) à un utilisateur, compte tenu de la sensibilité globale du rôle et le niveau du risque d'accès global de l'utilisateur.

Krausevitch et al. [62] présentent un modèle mathématique générale qui permet d'autoriser ou de refuser l'accès d'un sujet s_i à un objet en tenant compte de la probabilité qu'un sujet plus qualifié soit disponible et l'utilité de l'octroi ou du refus d'un accès à s_i.

Nissanke et Khayat [78] considèrent un ensemble partiellement ordonné des niveaux de risque. Ces niveaux de risque sont attribués aux permissions dans un système *RBAC*. Par conséquent, l'exécution d'une permission est considérée plus risquée qu'une autre sur la base de ces niveaux de risque. Ce travail présente également une approche pour la réorganisation de la hiérarchie de rôles en utilisant l'analyse de risques des permissions.

Dimmock et *al.* [30] ont étendu le modèle *RBAC* pour développer un modèle qui permet de prendre des décisions sur la base de la fiabilité des utilisateurs et le coût des actions.

Foukoue et al. [39] exploitent des métadonnées de sécurité et des bases de connaissances sémantiques qui capturent des concepts spécifiques afin de construire une logique qui permet un partage optimisé de l'information du risque.

Fouad et al. [41] présentent une méthode pour la minimisation du risque de divulgation de données à un certain seuil acceptable. Les auteurs formulent le problème de minimisation du risque comme un problème d'optimisation discrète. Un algorithme détermine les transformations optimales qui doivent être effectuées sur les données avant

qu'ils ne soient publiés. Ces transformations optimales tiennent compte à la fois du risque associé à la divulgation de données et du bénéfice.

Han et al. [46] proposent une approche qui permet d'évaluer le niveau de risque pour répondre à une demande d'accès et déterminer les mesures d'atténuation des risques appropriées. Cette approche permet de calculer des valeurs de risque pour renforcer la sécurité suite à la délégation d'un rôle. La logique floue est utilisée pour l'évaluation du risque.

Hu et al. [49] emploient la notion de risque pour surveiller et gérer les menaces de collaboration afin de faire face à l'incertitude des environnements distribués.

Molloy et al. [72] proposent l'utilisation des mécanismes du marché pour déterminer la tolérance et la répartition des risques des organisations. Ils montrent comment inciter les employés à faire les meilleurs choix pour l'organisation, les encourager à se comporter honnêtement. L'approche permet aussi d'identifier les employés malveillants.

Un rapport de *MITRE Corporation* [71] propose une approche d'évaluation du risque en trois phases :
La phase zéro quantifie le risque. La phase une impose des restrictions sur le montant maximum de risque que l'organisme est prêt à accepter pour un document donné. La phase deux utilise le risque quantifié pour le comparer au coût total du préjudice ou du dommage. Ainsi, en définissant des seuils de risque acceptable et en affectant des unités de coût à chaque transaction (requête d'accès), l'organisation peut limiter et contrôler les dommages.

Balepin et al. [5] présentent des approches qui permettent de donner des décisions non-binaires dans les systèmes de détection et de prévention d'intrusion. Ces systèmes répondent différemment aux attaques en fonction des niveaux de risque, contrairement aux systèmes *autoriser / refuser* traditionnels.

Molloy et al. [73] présentent une nouvelle architecture, dans le cadre du modèle *ABAC*, basée sur le risque et l'apprentissage automatique pour un *PDP local*, où une décision est d'abord donnée avec un niveau d'incertitude. Le compromis entre l'incertitude et l'utilité associée à cette décision est ensuite évalué pour déterminer si la décision peut être prise

localement ou nécessite la consultation du *PDP central* qui utilise l'une des trois méthodes suivantes :

- *Utilité espérée* : dans cette approche, la certitude de la décision est utilisée directement pour calculer l'utilité espérée et choisir la décision la plus utile.
- *Utilité ajustée du risque* : cette approche est basée sur la mitigation du risque des dommages.
- *Contraintes indépendantes du risque* : cette approche consiste à classer les décisions par ordre d'utilité et puis rejeter toute décision qui ne satisfait pas les contraintes du risque.

La principale contribution de ce travail consiste à montrer que l'apprentissage automatique peut être utilisé pour prendre des décisions en matière de sécurité.

Dans le contexte du modèle de *Bell-LaPadula*, *Crampton et al*. [26] présentent une méthode pour déterminer une décision d'accès inédite en utilisant l'historique des demandes d'accès, des décisions d'accès et les règles formelles de *Bell-LaPadula*. Une approche similaire pour le modèle *RBAC* est présentée dans [97].

Srivatsa et al.[89] présentent une approche qui permet de partager des informations de façon sécuritaire. Cette approche consiste à modeler des métadonnées de sécurité en tant qu'un demi-espace vectoriel (par opposition à un treillis utilisé dans une approche *MLS*). Ce travail présente des techniques permettant d'incorporer des attributs de métadonnées dynamiques (par exemple, une fonction sensible au temps) et des sémantiques de transformation de l'information.

Covington et al. [25] présentent le modèle généralisé de contrôle d'accès (*GRBAC*). Ce travail étend *RBAC* traditionnel en appliquant le concept de rôle à toutes les entités d'un système (Dans *RBAC*, le concept *rôle* est uniquement utilisé pour les sujets). *GRBAC* définit trois types de rôles : les *rôles des sujets*, les *rôles de l'environnement* et les *rôles des objets* et tient compte des informations de contexte dans la prise de décisions d'accès.

Diep et al. [29] proposent un modèle de contrôle d'accès basé sur le risque. Dans ce modèle, les informations de l'environnement sont utilisées pour l'évaluation des risques et

la prise des décisions d'accès. Les auteurs ont montré comment ce modèle pourrait être utilisé pour gérer le contrôle d'accès dans un hôpital.

Sun et al. [92] traitent le sujet des *menaces internes* en considérant des facteurs tels que la motivation qui est évaluée quantitativement. Les auteurs introduisent la notion de taux de fraude de l'utilisateur (*UF*) pour désigner la possibilité qu'un utilisateur spécifique commette une fraude.

Zhang et al. [103] utilisent les paramètres de contexte dans leur modèle de contrôle d'accès dynamique basé sur les rôles en présentant deux idées clés :

- Les privilèges d'accès d'un utilisateur doivent changer quand le contexte change.
- Une ressource doit ajuster ses autorisations d'accès lorsque les informations du système (la bande passante du réseau, l'utilisation du processeur, l'utilisation de la mémoire) changent.

4.10 Conclusion

Les travaux présentés dans ce chapitre présentent des méthodes différentes qui permettent d'estimer quantitativement ou qualitativement le risque dans les systèmes de contrôle d'accès, à l'exception du modèle *RADAC* qui donne un cadre général sans proposer une approche précise de calcul du risque. Ces méthodes de calcul du risque considèrent plusieurs facteurs tels que le contexte, les efforts de surveillance, les coûts des mesures de sécurité, le besoin opérationnel, etc. Certains de ces travaux présentent des cadres généraux pour la gestion du risque dans les systèmes de contrôle d'accès incluant des approches qui permettent de mitiger les risques non acceptables en déterminant les mesures de sécurité à mettre en place via les obligations.

Les travaux que nous avons présentés en détail dans ce chapitre sont les suivants :

1. *Contrôle d'accès adaptable basé sur le risque* (*RADAC*).
2. *RADAC pour ABAC*.
3. *Estimation du risque de dérogation aux politiques d'accès*.
4. *RBAC basé sur le risque*.

5. *Sécurité multi-niveaux floue*.
6. *Contrôle d'accès basé sur le risque pour les systèmes d'information de santé.*
7. *Systèmes de contrôle d'accès basés sur le risque établi sur des inférences floues*

Le *Tableau 8* compare ces différents travaux en tenant compte d'un ensemble de critères.

Approche	*Estimation*	*Modèle traditionnel*	*Estimation des mesures de sécurité mis en place*	*Besoin opérationnel*	*Obligations*	*Opérations*	*Objectif de sécurité*
RADAC	*Non applicable*	*Tous les modèles*	*Non*	*Oui*	*Non*	*Tous les accès*	*Sans distinction*
RADAC-UCON	*Non applicable*	*ABAC*	*Non*	*Oui*	*Oui*	*Tous les accès*	*Sans distinction*
Dérogation-RBAC	*Qualitative*	*RBAC*	*Non*	*Oui*	*Oui*	*Tous les accès*	*Sans distinction*
RBAC-risque	*Quantitative*	*RBAC*	*Non*	*Oui*	*Oui*	*Tous les accès*	*Sans distinction*
Multiniveaux- floue	*Quantitative*	*MLS*	*Non*	*Non*	*Oui*	*Lecture*	*Confidentialité*
Risque dans les systèmes de santé	*Quantitative*	*Tous les modèles*	*Non*	*Oui*	*Non*	*Tous les accès*	*Sans distinction*
Inférence floue	*Quantitative*	*MLS*	*Non*	*Non*	*Oui*	*Lecture*	*Confidentialité*

Tableau 8. Étude comparative des approches d'évaluation du risque d'accès

Dans le cadre de cette thèse, nous reprenons plusieurs concepts utilisés dans ces travaux et nous proposons des solutions pour éviter certaines de leurs limites. En effet, nous proposons une approche d'analyse de risque basée sur les flux de l'information qui permet d'estimer qualitativement le risque des requêtes d'accès. Cette approche sera transformée en une approche quantitative qui prend en considération les mesures de sécurité mises en place pour le calcul du risque. De plus, notre approche permet d'estimer le risque des requêtes d'accès en écriture et en lecture, et distingue le risque sur la confidentialité du risque sur l'intégrité, ce qui permet d'avoir des estimations plus adaptées au contexte.

Notons que notre approche peut être appliquée à tous les modèles de contrôle d'accès moyennant des légères modifications. La considération du besoin opérationnel peut être intégrée à notre approche en considérant le concept des catégories. La considération des obligations pour atténuer le risque est un autre aspect qui pourrait être facilement intégrée à notre approche. La considération du besoin opérationnel et des obligations ne seront pas abordés dans cette thèse et feront l'objet de nos travaux futurs.

Le chapitre suivant, présente une vue générale de l'approche que nous proposons pour le calcul du risque des requêtes d'accès.

Chapitre 5 : Approche de calcul du risque dans les systèmes de contrôle d'accès

5.1 Introduction

Dans ce chapitre, nous présentons un aperçu général de l'approche que nous proposons pour le calcul du risque des requêtes d'accès. Notre méthode peut être vue comme une approche de calcul du risque de la violation d'une politique de sécurité suite à l'autorisation d'une requête. Cela inclut les cas où un employé utilise ses accès légitimes pour divulguer des données sensibles à une tierce partie, altérer des données, etc.

Dans le chapitre 4, nous avons présenté plusieurs approches qui permettent de prendre en considération l'aspect du risque pour la prise des décisions du contrôle d'accès. En général ces méthodes proposent des évaluations du risque qui sont fixes après leur calcul. Dans cette thèse, nous proposons une méthode qui permet de prendre en considération des facteurs qui peuvent évoluer rapidement dans le temps comme les flux d'information entre les sujets et les objets, les mesures de réduction de la potentialité de la menace et les mesures de réduction de l'impact.

Cette approche qui fournit une *évaluation qualitative* et *quantitative* du risque permet d'améliorer la qualité des décisions d'accès prises et leur pertinence. Elle consiste à suivre un ensemble d'étapes que nous présentons brièvement dans ce chapitre et qui seront détaillées dans les chapitres suivants.

Ce chapitre est organisé de la façon suivante : dans la section *2*, nous présentons la motivation derrière une approche dynamique de calcul du risque. Ensuite, nous présentons des définitions génériques du risque, liées à la technologie de l'information dans la section *3*. Nous présentons notre approche globale d'évaluation du risque pour les systèmes de contrôle d'accès dans la section *4* et nous concluons dans la section *5* par discuter les contributions de notre approche et ses limitations.

5.2 Motivation

Dans les exemples que nous présentons dans cette thèse, nous utilisons la notation graphique présentée dans la *Figure 15*. Nous désignons par *flux d'information potentiel*, le flux d'information qui peut se produire suite à l'autorisation d'un accès.

Forme	***Signification***
	Objet
	Sujet
	Flux d'informations permis
	Flux d'informations non permis
	Flux d'informations potentiel

Figure 15. Légende

5.2.1 Évaluation du risque

Contrairement aux modèles de sécurité multi-niveaux traditionnels qui donnent des décisions d'accès prédéfinis, le modèle que nous proposons permet d'accepter des accès qui seraient refusés par ces modèles traditionnels. Prenons l'exemple d'une requête d'accès en *écriture* d'un sujet, qui a un niveau de confidentialité *Top Secret***,** à des données qui ont un niveau de confidentialité *Restreint*. Dans un système de contrôle d'accès traditionnel qui applique le modèle *BLP*, cet accès doit être refusé tel que nous pouvons le voir dans la *Figure 16(a*).

Dans le cas du système de contrôle d'accès basé sur le risque que nous proposons, une requête d'accès sera autorisée si le risque qui lui est associé est inférieur au niveau du risque acceptable et elle sera refusée dans le cas contraire, comme nous pouvons le voir dans la *Figure 16(b).*

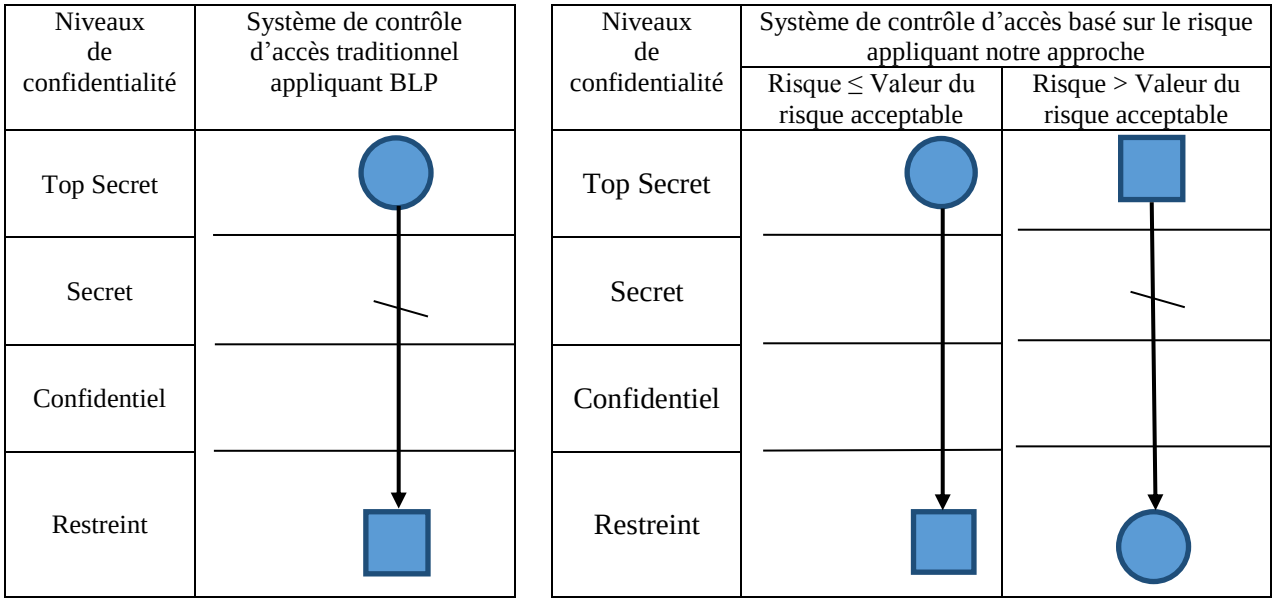


Figure 16. Contrôle d'accès traditionnel par opposition au Contrôle d'accès basé sur le risque

5.2.2 Application de l'évaluation du risque

Le contrôle d'accès basé sur le risque pourrait être utile pour déterminer quels employés peuvent accéder aux ressources dans le cadre de leur travail, le choix des objets à accéder dans le cadre d'un flux de travail, etc. En effet, les choix se porteront toujours sur le sujet ou l'objet qui représente le risque le moins élevé.

5.2.3 Approche dynamique

Une caractéristique intéressante de notre approche réside dans son aspect dynamique, en effet un accès accepté à un instant donné peut être refusé si le même accès est demandé à un instant ultérieur. De même, un accès refusé à un instant donné peut être accepté s'il est demandé à un instant ultérieur. Cela peut être le résultat du changement du niveau de sécurité du sujet et/ou du niveau de sécurité de l'objet, du niveau des mesures de sécurité réductrices du risque ou du changement du niveau de risque acceptable.

Dans la section suivante, nous présentons un ensemble de définitions du *risque lié à la technologie de l'information* que nous allons adapter aux systèmes de contrôle d'accès pour définir une fonction de calcul du risque des demandes d'accès.

5.3 Définitions du risque lié à la technologie de l'information

Cette section présente des définitions du *risque lié à la technologie de l'information* (*IT Risk*) en nous référant à des normes et standards qui font autorité dans ce domaine :

FIPS 200 [38] définit le risque comme « *le niveau d'impact sur les opérations de l'organisation (la mission, les fonctions, l'image ou la réputation), les actifs de l'organisation ou les personnes, résultant de l'exploitation d'un système d'information étant donné l'impact potentiel d'une menace et la probabilité que la menace se produise* ».

La norme *ISO* [56] définit le risque comme « *la probabilité d'une menace donnée d'exploiter les vulnérabilités d'un actif ou un groupe d'actifs et causer des dommages à l'organisation. Elle est mesurée en termes de combinaison de la probabilité d'occurrence d'un événement et de ses conséquences* ».

Dans la publication *NIST Special Publication 800-30* [90], le risque est défini comme « *une fonction de la probabilité qu'une menace exploite une vulnérabilité potentielle particulière, et l'incidence négative de cet événement sur l'organisation* ».

Selon *Méhari* [22], le risque est « *la conjonction d'un actif et d'une menace susceptible de faire un dommage à cet actif* ».

OWASP [79] définit le *risque R* comme étant le produit de la probabilité *L* d'un incident de sécurité et de l'impact *I* ($R = L \times I$).

D'après les définitions ci-dessus, le *risque lié à la technologie del'information* peut être vu comme étant fonction de la *potentialité de la menace* et de *l'impact*. Nous remarquons que la définition présentée dans [90] inclut le concept de *vulnérabilité* que nous n'avons pas utilisé explicitement dans notre approche puisque nous considérons qu'une *vulnérabilité* est le résultat du manque ou de l'absence des mesures de sécurité. Ce concept sera utilisé implicitement dans notre approche de calcul du risque.

5.4 Présentation de notre approche de calcul du risque

L'approche que nous présentons dans cette thèse traite les cas où un employé utilise ses accès légitimes pour effectuer une action qui viole la politique de sécurité : divulguer des données sensibles, fournir des renseignements à un employé qui n'a pas le droit de les connaître, etc. Elle consiste essentiellement à considérer le niveau de sécurité du sujet demandeur d'accès et le niveau de sécurité de l'objet à accéder pour déterminer la *potentialité de la menace* et l'*impact* d'une requête d'accès. Cette approche consiste à suivre les étapes suivantes représentées par la *Figure 17* :

1. calculer les *niveaux de sécurité des sujets et des objets* en considérant les flux d'informations générés par leurs accès passés,
2. calculer la *potentialité intrinsèque de la menace* et l'*impact intrinsèque*,
3. calculer la *potentialité de la menace* et l'*impact* en tenant compte des mesures de sécurité,
4. calculer le *risque* des accès demandés.

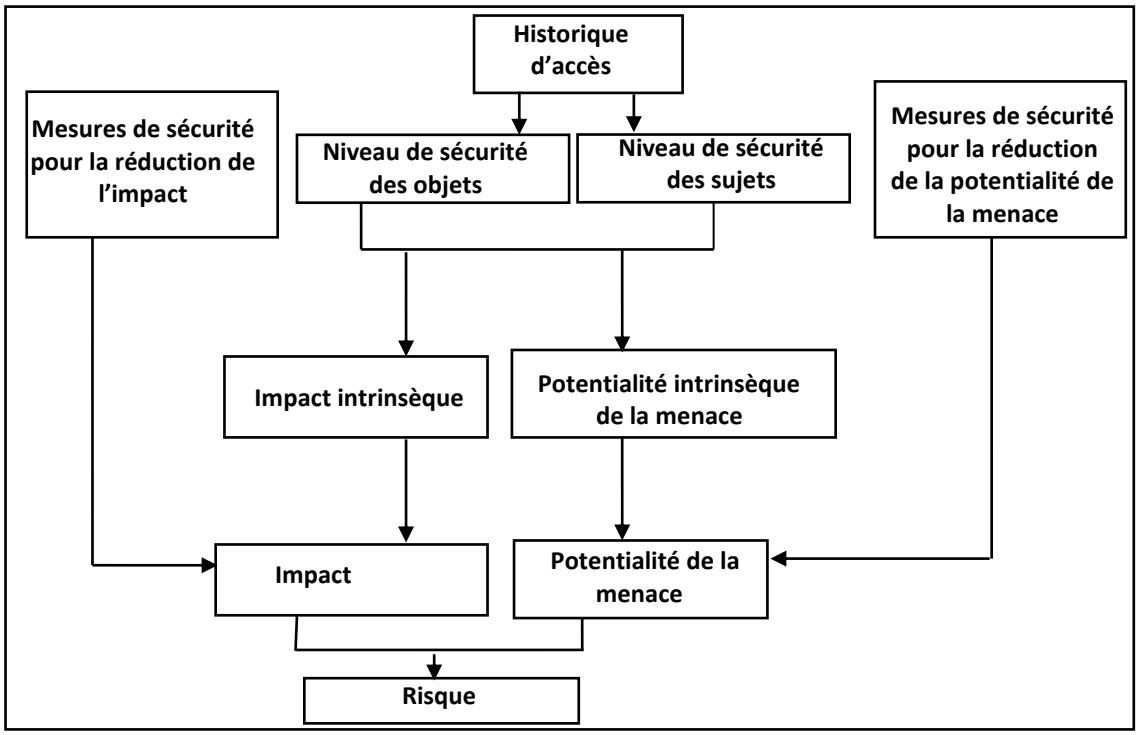


Figure 17. Approche de calcul du risque des requêtes d'accès

5.4.1 Calcul des niveaux de sécurité

La *Figure 18* représente la première étape de notre approche qui consiste à calculer les niveaux de sécurité des sujets et des objets en considérant leur historique d'accès. Cette étape fait l'objet du chapitre *6*.

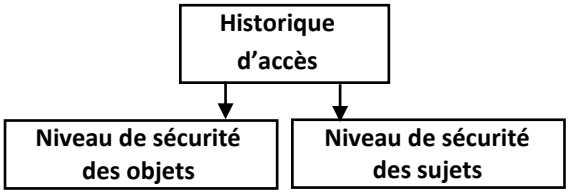


Figure 18. Calcul des niveaux de sécurité

L'intérêt de la considération de l'historique d'accès pour l'évaluation des niveaux de sécurité des sujets et des objets réside dans le fait que les accès précédents peuvent déterminer l'importance des informations connues par un sujet ou contenues dans un objet. Cela permet d'avoir des niveaux qui reflètent l'importance des informations qui pourraient être transmises entre les sujets et les objets. Ceci n'est pas possible dans le cas des niveaux statiques déterminés par défaut.

Discussion

À la différence de la méthode présentée dans [77] qui utilise la logique floue via l'attribution de degrés d'appartenance aux sujet et aux objets à chaque niveau de sécurité selon des fonctions prédéfinies (*Voir la section 8 du chapitre 4*), notre méthode se base sur les flux d'information résultant des accès passés pour le calcul des niveaux de sécurité. Nous croyons que notre procédé de calcul des niveaux de sécurité permet d'avoir des niveaux de sécurité qui reflètent mieux l'importance des informations connues par les sujets ou contenues dans les objets puisque les niveaux obtenues par notre méthode sont basées sur les flux d'informations et conséquemment évolutives dans le temps ce qui n'est pas le cas dans [77] où les niveaux de sécurité sont fixes une fois calculés.

5.4.2 Calcul de la potentialité intrinsèque de la menace

La *potentialité de la menace* représente, en quelque sorte, la possibilité de l'occurrence du risque, alors quela *potentialité intrinsèque* de *la menace* est une évaluation maximaliste de la possibilité de son occurrence, sans la considération des mesures de sécurité [23].

La *Figure 19* représente l'étape de calcul de la *potentialité intrinsèque de la menace* dans notre approche. L'intuition derrière le choix des niveaux de sécurité pour le calcul de la *potentialité intrinsèque de la menace* est que ces niveaux permettent de déterminer l'importance d'un flux d'informations résultant d'un accès. En effet, notre travail est basé sur l'hypothèse qui considère que la *potentialité intrinsèque de la menace* dépend de l'importance des flux d'informations entre les niveaux de sécurité des entités (sujets et objets). Autrement dit, nous définissons une *corrélation* entre le flux d'informations qui peut résulter d'un accès permis et la *potentialité intrinsèque de la menace*. La démarche complète de calcul de la *potentialité intrinsèque de la menace* sera amplement détaillée dans le chapitre *7*.

Dans cette thèse, nous allons définir des principes qui permettent de déterminer un *ordre de priorité* sur les *potentialités intrinsèques de menaces* des accès. Ces principes nous permettront par la suite de quantifier les *potentialités de menaces*.

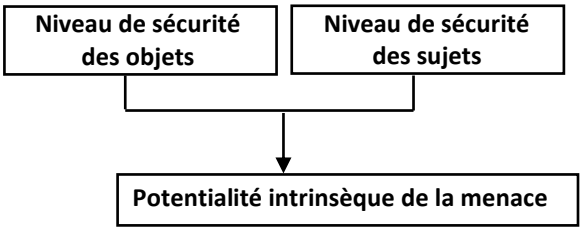


Figure 19.Calcul de la potentialité intrinsèque de la menace

5.4.3 Calcul de l'impact intrinsèque

La classification des données est la tâche d'évaluer leur importance pour qu'elles reçoivent un niveau de protection approprié. L'objectif principal de la classification des données est de classer les données d'une organisation par niveaux de sensibilité selon les objectifs de sécurité (la confidentialité, l'intégrité et la disponibilité). Le standard *FIPS 199* [37] et la

publication spéciale *NIST (SP) 800-60* [91] mentionnent que la classification des données est la première étape dans l'élaboration d'un cadre de gestion des risques. Le *Tableau 9* montre un exemple de classification de données basée sur les publications *FIPS 199* [37] et *NIST SP-800-60* [91], qui suggèrent que l'information soit classée en fonction des objectifs de sécurité et en utilisant des valeurs d'impact qualitatives, telles que *Faible*, *Modéré* et *Élevé*.

Objets	***Confidentialité***	***Intégrité***	***Disponibilité***
o_1	*N/A*	*N/A*	*N/A*
o_2	*Bas*	*Modéré*	*Élevé*
o_3	*Modéré*	*Modéré*	*Modéré*
o_4	*Élevé*	*Bas*	*Bas*
o_5	*Élevé*	*Élevé*	*Élevé*

Tableau 9. Niveaux d'impact selon FIPS 199 et NIST SP-800-60

Notons qu'aucune valeur d'impact n'a été définie pour les objectifs de sécurité de l'objet o_1 dans le *Tableau 9*. Cela nous permet de constater que o_1 est un objet non protégé qui a un niveau de classification *Non classé*. En règle générale, les valeurs d'impact d'un objet par rapport aux objectifs de sécurité sont précisées par les détenteurs des données dans une organisation. Une telle attribution de valeurs d'impact aux objets représente les dommages ou les pertes qui pourraient être causées à l'organisation ou à ses processus d'affaires lorsque les objectifs de sécurité sont compromis.

La définition des valeurs d'impact (*Faible*, *Modéré*, *Élevé)* est citée ci-dessous comme indiqué dans les publications *FIPS 199* [37] et *NIST SP-800-60* [91] :

- L'impact est faible si la perte de confidentialité, d'intégrité ou de disponibilité pourrait avoir un effet négatif limité sur les activités de l'organisation, les actifs de l'organisation ou les individus.
- L'impact est modéré si la perte de confidentialité, d'intégrité ou de disponibilité pourrait avoir un effet négatif important sur les activités de l'organisation, les actifs de l'organisation ou les individus.

- L’impact est élevé si la perte de confidentialité, d’intégrité ou de disponibilité pourrait avoir un effet indésirable grave ou catastrophique sur les opérations de l’organisation, les actifs de l’organisation ou des individus.

La *Figure 20* représente l’étape de notre approche qui consiste à calculer *l’impact intrinsèque* qui est une évaluation maximaliste des conséquences du risque, sans la considération des mesures de sécurité. Dans notre approche, *l’impact intrinsèque* est dépendant du niveau de sécurité de l’objet ou du sujet.

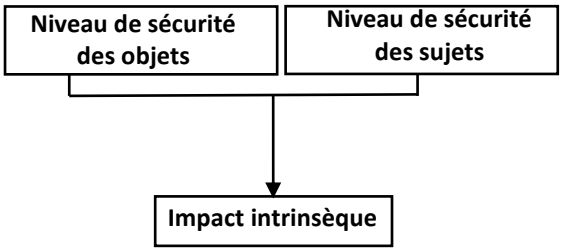


Figure 20. Calcul de l’impact intrinsèque

Pour calculer l*’impact intrinsèque* nous considèrons que dans le cas des accès de lecture vers le haut où l’objectif de confidentialité est visé et des accès de lecture vers le bas où l’objectif d’intégrité est visé, les informations sont transférées des objets vers les *sujets*. Ainsi, nous considérons que la valeur de *l’impact intrinsèque* dépend des niveaux de sécurité des objets. Dans le cas des accès d’écriture vers le bas où l’objectif de confidentialité est visé et des accès d’écriture vers le haut où l’objectif d’intégrité est visé, les informations sont transférées des sujets vers les objets. Ainsi, nous considérons que la valeur de *l’impact intrinsèque* dépend des niveaux de sécurité des *sujets*. En effet, l’*impact intrinsèque* dépend du niveau de sécurité de l’entité (sujet ou objet) source de l’information. *L’impact intrinsèque* est *proprtionnel* au niveau de l’entité source de l’information dans le cas de la confidentialité. Il est *inversement proprtionnel* au niveau de l’entité source de l’information dans le cas de l’intégrité. Par exemple, l’accès en écriture d’un sujet qui a un niveau de confidentialité *Top secret* peut avoir un impact plus grand que l’accès en écriture d’un sujet qui a un niveau de confidentialité *Secret*.

Le calcul de l’*impact intrinsèque* sera détaillé dans le chapitre *8.*

5.4.4 Calcul de la potentialité de la menace et de l'impact

Le *risque intrinsèque* résultant d'un accès permis est fonction de la potentialité *intrinsèque* de la menace et de l*'impact intrinsèque*. Ce *risque* peut être réduit par des mesures de sécurité.

La norme I*SO/CEI 27001* [56] exige une vérification régulière de la sécurité des systèmes d'information. Pour ce faire, l'administrateur de sécurité mesure l'effet des mesures de sécurité mises en place. Dans notre approche, nous adoptons des concepts de la méthodologie *Méhari* [23] pour intégrer l'évaluation des *mesures de sécurité* mises en place et qui sont des moyens de gérer le risque (des politiques, des procédures, des outils technologiques, etc.).

Soit l'exemple suivant qui consiste à considérer les deux cas suivants :

- Cas 1 : la demande d'accès dans un environnement où l'effet des mesures de sécurité mises en place est élevé (authentification forte, algorithme de chiffrement efficace, etc.).
- Cas 2 : la même demande d'accès de *Cas 1* dans un environnement où l'effet des mesures de sécurité mises en place est peu élevé.

Nous pouvons constater que le risque dans *Cas 1* serait moins élevé que celui dans *Cas 2*.

Nous distinguons deux grandes familles de mesures de sécurité :

1. Les mesures de sécurité qui permettent de réduire la *potentialité de la menace* (les mesures structurelles, les mesures dissuasives et les mesures préventives).
2. Les mesures de sécurité qui permettent de réduire l'*impact* (les mesures protectives, les mesures palliatives et les mesures récupératives).

Dans la section suivante, nous présentons plus en détail les catégories des mesures de sécurité.

5.4.4.1 Effet des mesures de sécurité

Dans le cadre de cette thèse, nous nous sommes inspirés de la base de connaissances de Méhari [22] et [23] afin de considérer l'effet des mesures de sécurité pour la réduction de

la *potentialité intrinsèque de la menace* ou *l'impact intrinsèque* du risque que pourrait représenter unaccès.

Le choix des mesures de sécurité et la détermination de leur contribution dans la réduction de la *potentialité de la menace* et de l'*impact* pourraient être déterminés par un expert en sécurité.

Exemple :

- La mesure *activation de la journalisation* permet de réduire la *potentialité de la menace* sur la confidentialité et sur l'intègrité lorsqu'un sujet accède à un objet.
- La mesure *copies de sauvegarde* permet de réduire l'impact sur l'intègrité lorsqu'un sujet accède à un objet.

La quantification de l'effet des mesures de sécurité dans la réduction de la *potentialité de la menace* et de l'*impact* sera discutée dans les chapitres *7* et *8*.

5.4.4.2 Calcul de la potentialité de la menace

Pour calculer la *potentialité de la menace* des requêtes d'accès, la méthode *Méhari* [22, 23] propose d'analyser préalablement les mesures de sécurité qui permettent de réduire la *potentialité de la menace*. Cette méthode distingue trois catégories de mesures de sécurité réductrices de la potentialité de la menace :

1. Les mesures *structurelles* : ces mesures diminuent l'exposition naturelle au risque. En effet, devant une situation de risque donnée qui pourrait être causée par l'autorisation d'un accès, les organisations ne sont pas égales. **Exemple** : une organisation qui traite et sauvegarde des renseignements personnels (hôpital, organisme gouvernemental, etc.) serait plus exposée au risque de divulgation des données, qu'une autre organisation qui ne sauvegarde que des données publiques.
2. Les mesures *dissuasives* : ces mesures diminuent les intentions d'agression et augmentent le danger du risque ressenti par l'auteur d'une agression volontaire (Plus le danger ressenti par l'auteur de l'agression est grand, moins probable est sa tentative). **Exemple :** la détection par activation de la journalisation des accès, l'authentification, les sanctions administratives, etc.

3. Les mesures *préventives* : ces mesures diminuent la possibilité du sinistre.

   Exemple : la sensibilisation des employés à la sécurité de l'information.

Dans notre approche, la valeur *de la réduction de la potentialité de la menace* dans le cas d'une requête d'accès désigne la somme des effets des mesures de sécurité réductrices de la *potentialité de la menace* à considérer pour cette requête. La potentialité *de la menace* dans notre approche peut être décrite comme suit : *Potentialité de la menace = Potentialité de la menace intrinsèque – Valeur de la réduction de la potentialité de la menace.* L'approche complète pour le calcul de la potentialité de la menace sera détaillée dans le chapitre *7*.

La *Figure 21* illustre notre approche complète pour le calcul de la potentialité de la menace.

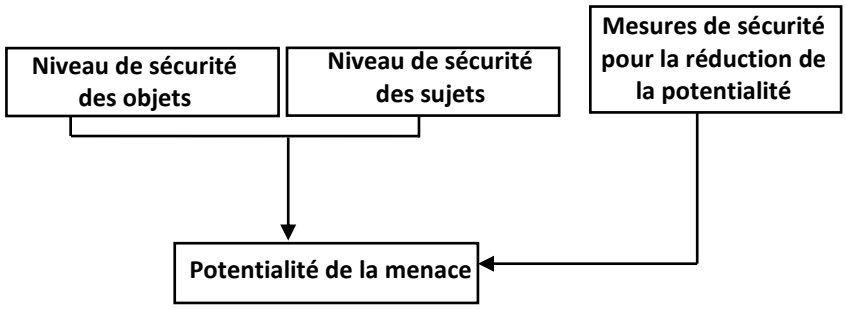


Figure 21. Calcul de la potentialité de la menace

Discussion

La *potentialité de la menace* est un intrant de l'évaluation du risque dans [7] et [20] : dans [7], la *vraisemblance de la menace* (*ThreatLikelihood),* définie comme la probabilité de la survenance d'un incident, est évaluée en utilisant la fonction ci-dessous où l'opérateur $\odot$ est défini par une matrice :

ThreatLikelihood (objective; role; extent) =
RoleThreat (role) $\odot$ *OpportunityThreat (objective; extent)*

Contrairement à l'*évaluation qualitative* de la potentialité dans *RBAC* présentée dans [7], nous présentons dans cette thèse une évaluation qualitative et quantitative basée sur le flux d'information et applicable à plusieurs modèles de contrôle d'accès. De plus, notre évaluation de la potentialité ne se limite pas aux accès en lecture et aux menaces sur la

confidentialité comme c'est le cas dans [20], mais elle s'étend aux accès en écriture et aux menaces sur l'intégrité. De surcroît, nous considérons l'effet des mesures de sécurité pour le calcul de la *potentialité de la menace* ce qui n'est pas le cas dans [7] et [20].

5.4.4.3 Calcul de l'impact

Nous avons présenté brièvement dans la section 5.4.3 notre approche pour le calcul de l'*impact intrinsèque* qui est une évaluation maximaliste des conséquences du risque, en dehors de toute mesure de sécurité. Dans notre approche, l'*impact intrinsèque* est déterminé par les niveaux de sécurité des objets ou des sujets et représente un préalable pour le calcul de l'*impact*.

Dans cette section, nous présentons notre approche pour le calcul de l'*impact* qui représente la gravité des conséquences directes et indirectes qui découleraient de l'occurrence du risque. L'occurrence du risque étant la divulgation, ou l'altération de données [23].

Le calcul de l'*impact* d'un accès passe par l'évaluation de l'effet des mesures d'atténuation de l'*impact*. *Méhari* [22, 23] distingue trois catégories de ces mesures de sécurité :

1. Les mesures *protectives* : ces mesures réduisent les conséquences directes d'un risque qui peuvent s'étendre et se propager. Moins ces conséquences sont confinées, plus le risque est grand. **Exemple** : les mesures de détection (activation de la journalisation des accès) qui permettent une réaction rapide face à un incident de sécurité.
2. Les mesures *palliatives* : ces mesures limitent les conséquences indirectes d'un risque. En effet la situation de crise engendrée par l'occurrence d'un risque peut être anticipée et préparée. Moins cette situation de crise est préparée, plus le risque est grand. **Exemple** : les copies de sauvegarde.
3. Les mesures *récupératives* : ces mesures permettent de reduire l'impact des pertes finales. **Exemple** : analyse spécifique des risques à couvrir par l'assurance et préparation spécifique des actions en justice.

L'e*ffet de la réduction de l'impact* dans le cas d'une requête d'accès désigne la somme des effets des mesures de sécurité réductrices de l'*impact* à considérer dans le cas de cette requête. Dans notre approche, l'impact est décrit comme suit : *Impact = Impact intrinsèque – Effet de la réduction de l'impact*. L'approche complète pour le calcul de l'impact sera détaillée dans le chapitre *8.*

La *Figure 22* illustre notre approche complète pour le calcul de l'*impact*.

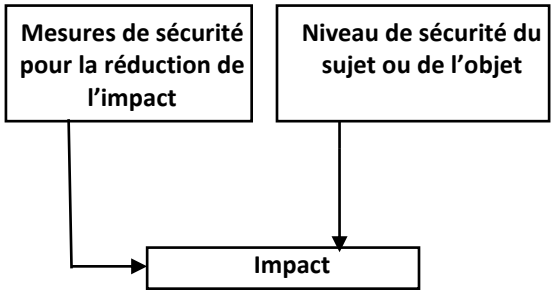


Figure 22. Calcul de l'impact

Discussion

Dans [7], le besoin de protection est égal à l'évaluation de l'impact de la perte de confidentialité, d'intégrité ou de disponibilité. Dans [20], la « valeur » de l'information est égale à l'évaluation du préjudice subi si cette information lue est divulguée d'une façon non autorisée. Tel que mentionné dans la section *5.4.3*, la valeur de l'*impact* dans notre approche dépend de l'action demandée et de l'objectif de sécurité visé.

L'approche que nous proposons pour le calcul de l'*impact intrinsèque* qui est un préalable pour le calcul de l'*impact*, considère que la valeur d'*impact intrinsèque* est proportionnelle au niveau de sécurité de l'entité source de l'information. Nous croyons que notre approche est plus pertinente que celles présentées dans [7] et [20] puisque nous considérons des niveaux de sécurité dynamiques qui reflètent le contenu des objets et les informations connues par les sujets. De surcroît, nous considérons l'effet des mesures de sécurité pour le calcul de l'impact ce qui n'est pas le cas dans [7] et [20].

5.4.5 Calcul du risque

En tenant compte des références citées dans la section *5.3*, nous décrivons le risque dans notre approche comme suit : *Risque = Potentialite de la Menace × Impact*.

Discussion

Dans certains travaux qui ont traité le sujet de l'évaluation du risque dans les systèmes de contrôle d'accès, certaines formules ont été proposées. En effet, dans [7] le risque est estimé pour chaque objectif de sécurité (confidentialité, intégrité et disponibilité), le risque spécifique *SpecificRISK* est estimé par la formule suivante où l'opérateur $\otimes$ est défini par une matrice.

SpecificRisk (objective; role; extent) =   *ThreatLikelihood (objective; role; extent)* $\otimes$ *ProtectionNeed(objective; extent)*

L'évaluation du *risque spécifique* passe par l'évaluation du *besoin de protection* (*ProtectionNeed)* et de la *vraisemblance de la menace* (*ThreatLikelihood).* Le besoin de protection est déterminé par l'évaluation de l'impact de la perte de confidentialité, d'intégrité ou de disponibilité.

Dans [20], le risque d'un accès en lecture est défini par la formule suivante : *Risque = (probabilité du préjudice) × (valeur de l'information)***.** La « valeur » de l'information est définie comme le préjudice subi si cette information accédée, est divulguée d'une façon non autorisée.

Contrairement à la formule présentée dans [7], notre formule permettra de quantifier le risque et ne se limitera pas à une évaluation qualitative. De plus, notre approche pour le calcul de la *potentialité de la menace* est différente de l'approche de calcul de la *probabilité du préjudice* dans [20] (*Voir la section 6 du chapitre 4*).

Notre approche permettra de quantifier le risque pour les accès en lecture et en écriture contrairement à la formule présentée dans [30] qui se limite au calcul du risque des accès en lecture interdits par *Bell-LaPadula*. De plus, notre approche sera applicable à l'objectif de l'intégrité et ne se limitera pas à la confidentialité et prendra en considération l'effet des mesures de sécurité mises en place.

La *Figure 23* représente l'étape de calcul du risque à partir des valeurs de la potentialité et de l'impact obtenus dans les étapes précédentes. Ainsi, et tel que le montre la *Figure 17* présentée dans la section *5.4*, en suivant toutes les étapes citées dans ce chapitre, nous serons en mesure de calculer le risque d'une requête d'accès.

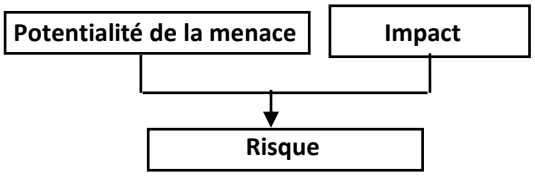


Figure 23. Calcul du risque en fonction de la potentialité de la menace et de l'impact

5.5 Conclusion

L'approche de calcul du risque des requêtes d'accès que nous présentons dans cette thèse traite les cas où un sujet dans une organisation (p. ex. un employé) utilise ses accès légitimes pour effectuer une action qui viole la politique de sécurité. Notre méthode permet de calculer le risque de la violation d'une politique de sécurité suite à l'autorisation d'une requête d'accès. Cette approche est caractérisée par son aspect dynamique puisque son application implique le changement des décisions d'accès en fonction de l'historique des accès du sujet demandeur d'accès et de l'objet auquel l'accès est demandé. De plus, notre approche tient compte de l'effet des mesures de sécurité mises en place ce qui permet d'obtenir des valeurs de risque plus réalistes. Ainsi, notre approche qui fournit une *évaluation qualitative* et *quantitative* du risque permet d'améliorer la qualité des décisions d'accès prises et leur pertinence.

5.5.1 Étapes de notre approche

L'approche de calcul du risque que nous avons proposée dans ce chapitre consiste à suivre un ensemble d'étapes.

La première étape consiste à appliquer une approche qui tient compte de l'historique des accès pour calculer les niveaux de sécurité des sujets et des objets. À cet effet, des *formules* pour le calcul de ces niveaux sont développées dans cette thèse.

Pour appliquer la deuxième et la troisième étape de notre approche, nous définissons des principes pour calculer les *potentialités des menaces* des accès et de leurs *impacts*. Ces principes se basent sur les niveaux de sécurité des sujets et des objets et considèrent les mesures de sécurité réductrice de la *potentialité de la menace* et de l'*impact*. Des *formules* pour le calcul des potentialités de menaces des accès et de leurs impacts sont développées dans cette thèse.

La dernière étape de notre approche consiste à déterminer la valeur du risque. À cet effet, nous avons adopté une formule de calcul du risque en nous inspirant des standards faisant autorité dans le domaine de l'évaluation des risques liés à la technologie de l'information.

5.5.2 Limites de notre approche

Cette approche ne permet pas d'estimer le risque sur la *disponibilité* et se limite à la *confidentialité* et à l'*intégrité*. De plus, elle se restreint aux opérations de lecture et d'écriture et ne permet pas d'estimer le risque d'autres opérations. En outre, notre approche ne permet pas l'évaluation des risques d'*ingénierie sociale* [45] et de *déni de service* [1].

Chapitre 6 : Calcul des niveaux de sécurité des sujets et des objets

6.1 Introduction

Les données des organisations doivent être protégées pour assurer leur confidentialité, leur intégrité et leur disponibilité. Pour ce faire, des niveaux de *classification* (*Non classé*, *Restreint*, *Confidentiel*, *Secret*, *Top secret*) sont attribués aux objets (fichiers, bases de données, etc.) afin de refléter l'importance des données qu'ils contiennent et le niveau adéquat des mesures de sécurité à mettre en place pour les protéger. De plus, l'accès à ces objets est restreint par des politiques de sécurité à des sujets (processus, machines, etc.) bien déterminés. Ainsi, une côte de sécurité (*habilitation*) est requise pour déterminer les données auxquelles un sujet peut accéder.

Les modèles de contrôle d'accès multi-niveaux (*MLS*) (dont le plus connu est le modèle *Bell-LaPadula* (*BLP*) [8]) permettent de contrôler les flux d'informations en utilisant les niveaux de sécurité. Cependant, ces modèles sont rigides et peu pratiques dans des environnements dynamiques.

Le contrôle d'accès basé sur les rôles (*RBAC*) et ses variantes [3, 34, 35, 36, 84] sont couramment utilisés, cependant ce modèle ne prévoit ni la classification des informations, ni des mécanismes explicites de contrôle de flux. Ainsi, des données hautement classifiées peuvent passer à des niveaux moins élevés.

Le contrôle d'accès basé sur les attributs (*ABAC*) [51] permet de spécifier des niveaux de sécurité mais sans offrir des mécanismes qui permettent leur utilisation efficace. Nous pensons qu'un système de contrôle d'accès doit intégrer des mécanismes qui permettent l'ajustement dynamique des niveaux de sécurité pour refléter les changements dans l'environnement. *ABAC* et les modèles *MLS* classiques utilisent des niveaux statiques définis à l'initialisation du système.

La contribution principale de ce chapitre consiste à proposer une approche qui permet de déterminer dynamiquement un *ordre de priorité* sur les niveaux de sécurité des sujets et des objets tout en tenant compte des inférences d'informations (association et agrégation

d'informations) et leurs conséquences lorsque l'objectif de confidentialité est visé. Nous proposons également des formules qui permettent de calculer des niveaux de sécurité (confidentialité et intégrité). L'application de cette approche représente la première étape de notre méthode de calcul du risque des requêtes d'accès, qui se base, principalement, sur les niveaux de sécurité.

Le reste de ce chapitre est organisé comme suit : dans la section *2*, nous présentons des exemples pour motiver la problématique. La section *3* présente un ensemble de concepts de base. Les sections *4*, *5* et *6* présentent des principes pour le calcul des niveaux de confidentialité. La section 7 présente des formules de calcul des niveaux de confidentialité. La section *8* présente des principes et des formules pour le calcul des niveaux d'intégrité. Dans la section 9, nous expliquons comment appliquer notre approche de calcul des niveaux de sécurité au modèle de contrôle d'accès *ABAC* [51]. La section *10* présente un tableau qui récapitule toutes les notations utilisées dans ce chapitre. Dans la section *11*, nous comparons notre travail avec des travaux connexes. Finalement, dans la section *12*, nous récapitulons nos contributions et nous discutons les limites de notre approche.

Notons qu'une partie du travail présenté dans ce chapitre a fait l'objet de la publication [12].

6.2 Motivation

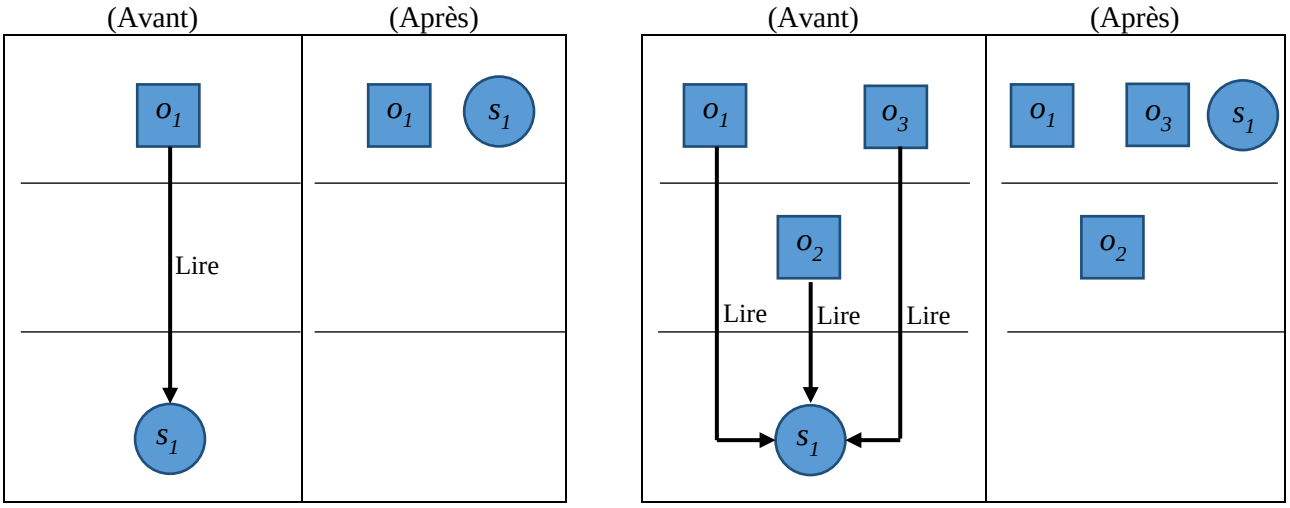
Dans le présent travail, nous considérons les modèles de contrôle d'accès, où les accès sont contraints par des règles de contrôle, basées sur les niveaux de sécurité. Par ailleurs, nous supposons que des exceptions au contrôle d'accès établi sont possibles suite, par exemple, à une analyse de risque. L'exception peut être accordée par un administrateur ou par des règles appliquées systématiquement.

Un flux d'informations est un transfert d'informations entre entités (sujets et objets). Certains flux d'informations sont plus importants que d'autres, en raison de leurs conséquences possibles. Par exemple, un flux d'informations d'un sujet *Top secret* qui écrit dans un objet *Non classé* implique le stockage d'informations *Top secret* dans un objet probablement accessible par tous. Dans ce cas, des informations *Top secret* pourraient être

divulguées au public si ce flux d'informations n'est pas pris en considération lors de la détermination des décisions d'accès.

À notre connaissance, seulement deux modèles de contrôle d'accès connus dans la littérature, sont basés sur les flux d'informations pour définir des règles de mise à jour des niveaux de sécurité : le modèle du *plus haut niveau* (*high water mark*) [98], qui est une extension de *Bell-LaPadula* [8] et le modèle du *plus bas niveau* (*low water mark*) [98] qui est une extension du modèle *Biba* [9]. Ces modèles, connus sous les noms de *modèles de sécurité multi-niveaux* (*MLS*) et que nous avons présentés dans le chapitre *3*, seront discutés dans la section *8*.

Prenons les deux exemples de la *Figure 24* qui représentent l'attribution des niveaux de confidentialité selon le modèle du *plus haut niveau* (*High water mark*). Dans l'**Exemple 1**, le sujet s_1 a lu un seul objet ayant un niveau supérieur au sien (o_1). Dans l'**Exemple 2**, s_1 a lu trois objets ayant des niveaux supérieurs au sien (o_1, o_2, o_3). Nous remarquons que dans ces deux exemples, le sujet s_1 obtient le même niveau de confidentialité puisque seul le plus haut niveau de confidentialité des objets lus, est considéré. En effet, les niveaux de confidentialité sous ce modèle ne dépendent pas du nombre des flux passés et de leurs conséquences. Cependant, nous devrions nous attendre à ce que trois accès en lecture à des objets différents ayant un niveau de confidentialité supérieur au niveau du sujet, permettent à ce dernier de connaître plus d'informations qu'un accès en lecture à un seul objet ayant le même niveau de confidentialité supérieur au niveau du sujet. Cela nous mène à conclure que les niveaux de confidentialité attribués sous ce modèle ne reflètent pas bien l'importance des informations qui pourraient être connues par les sujets ou contenues dans les objets. D'où l'intérêt de définir un modèle qui permet de pallier à ces limites.



Exemple 1 ***Exemple 2***

Figure 24. Limites du modèle du plus haut niveau

Nous verrons dans ce chapitre également que des informations peuvent non seulement être reçues, mais aussi être déduites par inférence. Cela peut représenter une faille de sécurité si des informations hautement classifiées peuvent être déduites à partir d'informations moins classifiées [31, 32, 33, 85]. Par exemple, et comme nous pouvons le voir dans la *Figure 25*, les deux objets à l'intérieur du cercle ont un niveau de confidentialité *4*, même si le niveau de chaque objet considéré séparément est inférieur à *4*. L'objet ayant le niveau de confidentialité *1* représente un texte chiffré, l'objet ayant le niveau de confidentialité *3* représente la clé de chiffrement. La combinaison du contenu de ces deux objets permet d'obtenir le texte déchiffré qui a un niveau de confidentialité *4*. D'autres exemples qui illustrent ce cas sont présentés à la section *6.4.1.1*.

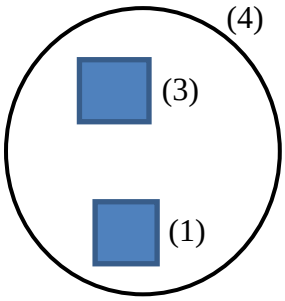


Figure 25. Inférence

Dans la section suivante, nous présentons des concepts de base nécessaires pour la compréhension de l'approche que nous proposons.

6.3 Concepts de base

Nous supposons l'existence des ensembles suivants : S un ensemble de sujets, O un ensemble d'objets, E un ensemble d'entités tel que $E = S \cup O$, I un ensemble d'informations, L_c un ensemble de niveaux de confidentialité, L_i un ensemble de niveaux d'intégrité et T un ensemble d'instants (valeurs discrètes du temps). Les éléments de ces ensembles sont désignés respectivement par des lettres minuscules s, o, e, it, l_c, l_i et t. Nous définissons un ordre total sur T représentant l'ordre temporel.

Selon [83] et [67], la confidentialité est liée à la divulgation de l'information, tandis que l'intégrité est liée à sa modification. Dans notre approche, nous considérons que lorsque les sujets et les objets reçoivent des informations, leurs niveaux de confidentialité peuvent augmenter alors que leurs niveaux d'intégrité peuvent diminuer. Ces idées sont derrière les propriétés des modèles *MLS* (*BLP* et *BIBA*), ainsi que des modèles *HWM* et *LWM* (Voir chapitre *2*).

Nous considérons que le transfert des informations entre sujets et objets peut provoquer le changement des niveaux de sécurité. Ces transferts d'informations peuvent être le résultat d'opérations de lecture, d'écriture ou d'inférences. Tous nos exemples se réfèreront à ces cas même si le transfert d'informations peut être possible à travers des canaux cachés. Nous soulignons que nos définitions sont basées sur les trois hypothèses suivantes (Hypothèses pessimistes) [50] :

- la lecture d'un objet par un sujet implique le transfert de toutes les informations contenues dans l'objet vers le sujet,
- l'écriture dans un objet par un sujet implique le transfert de toutes les informations connues par le sujet vers l'objet,
- l'information ne peut pas être effacée, c'est-à-dire si un sujet connaît une information ou un objet contient une information à un instant donné, il continue à la connaître ou à la contenir à tous les instants suivants.

Nous adaptons les concepts suivants présentés dans [60] comme suit :

- Deux relations *Know (Kn)* et *Store (St)*.

- Deux relations qui expriment les accès précédents entre les sujets et les objets: *HasRead HR* et *HasWritten HW*.

Les règles d'inférence pour *Kn* sont les suivantes :

- $HR(s, o, t) \rightarrow Kn(s, o, t)$ (si *s* a lu *o* à l'instant *t*, alors *s* connaît l'information de *o* à partir du même instant *t*).
- $HW(s', o, t) \wedge HR(s, o, t') \wedge (t \leq t') \rightarrow Kn(s, s', t') \wedge Kn(s, o, t')$ (si *s'* a écrit dans *o* à l'instant *t* et *s* lit de *o* à l'instant *t'* tel que *t'* est un instant postérieur à *t*, alors *s* connait l'information de *s'* et de *o* à partir de l'instant *t'*).
- $Kn(s, s, t)$ est toujours vrai.

Les règles d'inférence pour *St* sont les suivantes :

- $HW(s, o, t) \rightarrow St(o, s, t)$ (si s a écrit dans o à l'instant t, alors o contient l'information connu par s à partir du même instant t).
- $HR(s, o, t) \wedge HW(s, o', t') \wedge (t \leq t') \rightarrow St(o', o, t') \wedge St(o', s, t')$ (si s a lu de o à l'instant t et s écrit dans o' à l'instant t' tel que t' est un instant postérieur à t, alors o' contient l'information de o et de s à partir de l'instant t').
- $St(o, o, t)$ est toujours vrai.

Les seules relations *Kn* ou *St* qui peuvent exister dans un système sont celles qui peuvent être déduites par les règles précédentes. Nous définissons également les fonctions *StS* et *KnS* comme suit :

- *KnowSet(s, t')* noté $KnS(s, t')$ est l'ensemble d'entités *e* pour lesquelles il existe $t \leq t'$ et $Kn(s, e, t)$ est vrai : $KnS(s, t') = \{e \mid t \leq t', Kn(s, e, t) = vrai\}$.
- *StoreSet (o, t')* noté $StS(o, t')$ est l'ensemble d'entités *e* pour lesquelles il existe $t \leq t'$ et $St(o, e, t)$ est vrai : $StS(o, t') = \{e \mid t \leq t', St(o, e, t) = vrai\}$.

Nous considérons aussi que le nombre d'entités dans $KnS(s, t)$ représente le nombre de flux d'informations reçus par le sujet *s* jusqu'à l'instant *t*, et que le nombre d'entités dans $StS(o, t)$ représente le nombre de flux d'informations reçus par l'objet *o* jusqu'à l'instant *t*.

L'exemple suivant introduit l'idée de notre approche. Considérons un système avec deux sujets s_1 et s_2, deux objets o_1 et o_2 et trois instants t, t' et t'' avec $t < t' < t''$. Supposons que seuls les accès suivants ont été effectués :

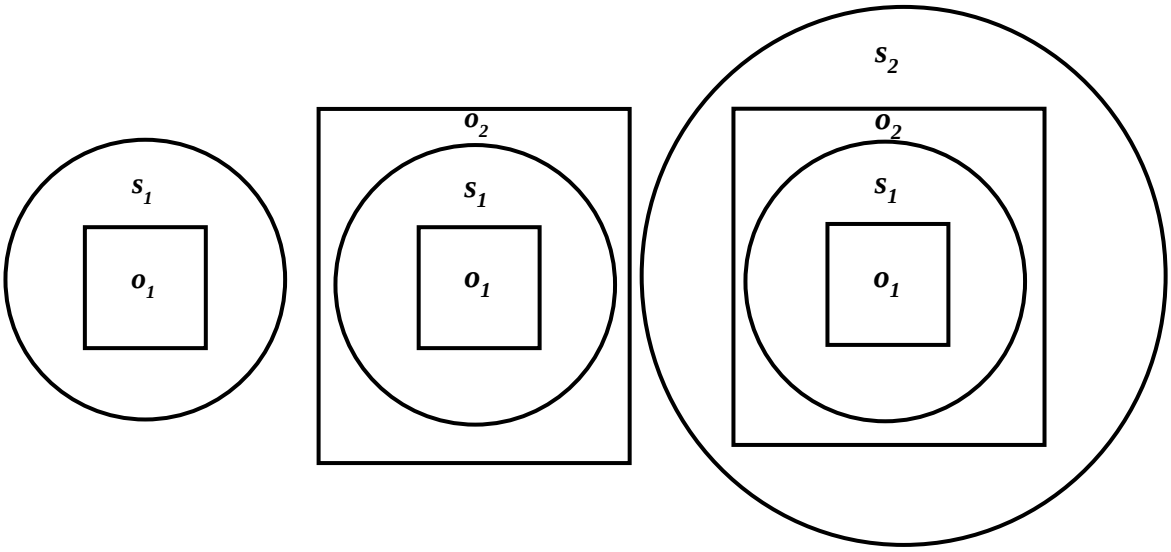
a. $HR(s_1, o_1, t)$: s_1 a lu o_1 à l'instant t.

b. $HW(s_1, o_2, t')$: s_1 a écrit dans o_2 à l'instant t'.

c. $HR(s_2, o_2, t'')$: s_2 a lu o_2 à l'instant t''.

D'après a, b et c, nous pouvons déduire que $KnS(s_1, t) = \{s_1, o_1\}$, $StS(o_2, t') = \{s_1, o_1, o_2\}$ et $KnS(s_2, t'') = \{s_1, o_1, o_2, s_2\}$. En d'autres termes, les sujets connaissent des informations en les lisant à partir des objets et les objets contiennent des informations transférées par des sujets qui les écrivent dans ces mêmes objets.

Les effets des étapes *a*, *b* et *c* de l'exemple précédent, sont présentés dans la *Figure 26*, où les sujets sont représentés par des cercles et les objets par des rectangles. Un cercle contenant un rectangle signifie qu'un sujet connaît les informations contenues dans un objet. Un cercle contenant un cercle signifie qu'un sujet connaît les informations d'un autre sujet. Un rectangle contenant un cercle signifie qu'un objet contient les informations d'un sujet. Un rectangle contenant un rectangle signifie qu'un objet contient les informations d'un autre objet.



(a) (b) (c)

Figure 26. Effets de a, b et c

La *Figure 26(a)* montre que s_1 connaît les informations de o_1, en plus de ses propres informations. La *Figure 26(b)* montre que o_2 contient les informations de s_1 *et* o_1, en plus de ses propres informations. La *Figure 26(c)* montre que s_2 connaît les informations de s_1, o_1 et o_2, en plus de ses propres informations.

6.4 Évaluation des niveaux de confidentialité basée sur les flux d'informations

Tout au long de cette section, nous présentons une série d'exemples pour introduire les fondements conceptuels de notre approche d'évaluation des niveaux de confidentialité. L'idée de base de notre approche consiste à considérer qu'initialement des niveaux de confidentialité sont attribués aux sujets et aux objets et que ces niveaux changent dynamiquement comme conséquence des flux d'informations entre les entités.

Nous définissons un ordre total sur l'ensemble des des niveaux de confidentialité L_c et pour chaque niveau, nous attribuons une valeur numérique respectant l'ordre défini. Par exemple, si L_c = *{Non classé, Restreint, Secret, Top Secret}*, alors la valeur attribuée à *Non classé* est *1*, celle attribuée à *Restreint* est *2* et ainsi de suite. Pour simplifier la notation,

nous considérons qu'il n'y a qu'un seul ensemble L_c qui s'applique aux sujets, aux objets et aux informations.

Dans ce qui suit, nous utilisons les *multiensembles* pour déterminer les niveaux de sécurité des sujets et des objets. Le concept de *multiensemble* est une généralisation de la notion d'ensemble, de sorte qu'il permet des occurrences multiples d'éléments identiques. Formellement, un *multiensemble* est une *paire* (L_c, m) où L_c est le *support* et $m: L_c \rightarrow N$ est la *fonction de multiplicité* où N est l'ensemble des entiers naturels. Donc, dans le *multiensemble* (L_c, m), l'élément x apparaît $m(x)$ fois. **Exemple** : $\{1, 2, 1, 2, 2, 4\}$ est le multiensemble $(\{1, 2, 3, 4, 5\}, m)$ où m est la fonction telle que $m(1) = 2$, $m(2) = 3$, $m(3) = 0$, $m(4) = 1$ et $m(5) = 0$.

Les fonctions suivantes sont nécessaires pour développer notre approche :

- $csl(s, t)$ dénote le niveau de confidentialité d'un sujet s à l'instant t.
- $col(o, t)$ dénote le niveau de confidentialité d'un objet o à l'instant t.
- $cel(e, t)$ dénote le niveau de confidentialité d'une entité e à l'instant t.
- $cil(it)$ dénote le niveau de confidentialité d'une information it.
- $csl(s, t_0)$ et $col(o, t_0)$ dénotent respectivement les niveaux de confidentialité initiaux du sujet s et de l'objet o.
- $KnSL_c(s, t')$ est le multiensemble des niveaux initiaux des entités e dont le contenu est connu par s (c.-à-d $\forall t \leq t'$ tel que $Kn(s, e, t)$ est vrai). **Exemple** : **s**upposons que $csl(s, t_0) = l_c'$. $KnSL_c(s, t) = \{l_c', l_c', l_c, l_c'\}$ signifie qu'à l'instant t, le sujet s de niveau initial l_c' connaît ses informations, les informations de deux entités différentes ayant chacun un niveau initial l_c' et les informations d'une troisième entité ayant un niveau initial l_c.

La définition de ce multiensemble nous permettra d'évaluer les niveaux de confidentialité des sujets, en fonction de leurs accès précédents en lecture ou plus généralement en fonction des flux d'informations reçus.

6.4.1 Évaluation des niveaux de confidentialité des sujets

Tel que mentionné précédemment, une hypothèse principale de notre travail stipule que les niveaux de confidentialité des sujets peuvent être calculés en considérant leur historique d'accès en lecture. Nous développons cette hypothèse en présentant un ensemble de principes intuitifs :

Principe 1 **:** le *niveau de confidentialité d'un sujet* qui n'a pas reçu de flux d'informations d'autres entités, est défini par défaut. Ce niveau peut être déterminé par l'administrateur de sécurité.

Principe 2 **:** plus les *niveaux de confidentialité* des entités, à partir desquelles un sujet a reçu des flux d'informations, augmente, plus *son niveau de confidentialité* augmente. Autrement dit, plus les niveaux de confidentialité initiaux des entités appartenant à *KnS(s, t)* augmentent, plus *csl(s, t)* augmente.

Principe 3 **:** plus le *nombre de flux d'informations* reçus par un sujet augmente, plus *son niveau de confidentialité* augmente. Autrement dit, plus le nombre d'entités appartenant à *KnS(s, t)* augmente, plus *csl(s, t)* augmente.

Scénario motivant **:** ci-après, nous présentons un scénario qui sera utilisé dans le reste du chapitre pour motiver notre approche. Le *Tableau 10(a)* montre les niveaux de confidentialité des sujets *Nadia*, *Claude*, *Bruno*, *Carl* et *Sabrina* à l'instant t_0. Le *Tableau 10(b)* montre les niveaux de confidentialité des objets o_1, o_2, o_3, o_4, o_5, o_6, o_7 et o_8 à l'instant t_0.

Nous supposons que seuls les accès que nous présentons ont été effectués et que les niveaux des sujets et des objets ne changent que sous l'effet de ces accès.

Sujet	*Niveau de confidentialité à l'instant t_0*
Nadia	*4*
Claude	*2*
Bruno	*1*
Carl	*1*
Sabrina	*1*

(a)

Objet	*Niveau de confidentialité à l'instant t_0*
o_1	*4*
o_2	*4*
o_3	*2*
o_4	*2*
o_5	*1*
o_6	*1*
o_7	*1*
o_8	*1*

(b)

Tableau 10. Niveaux de confidentialité

Exemple 1 : d'après le *Tableau 10*, nous avons ce qui suit : *csl(Bruno, t_0) = 1, csl(Carl, t_0) = 1, col(o_1, t_0) = 4* et *col(o_4, t_0) = 2*.

Supposons que *Bruno* a lu des informations de l'objet o_1 et *Carl* a lu des informations de l'objet o_4. Conformément au ***Principe 2***, le *niveau de confidentialité de Bruno* devient *supérieur* au *niveau de confidentialité de Carl.* Cela s'explique par le fait que le niveau de confidentialité de l'objet lu par *Bruno* est supérieur au niveau de l'objet lu par *Carl*.

Dans cet exemple, nous étions en mesure de comparer les niveaux de confidentialité de deux sujets en comparant les niveaux des objets qu'ils ont lus. Cependant, le ***Principe 2*** n'est plus suffisant lorsque les niveaux de confidentialité de ces objets sont les mêmes.

Exemple 2 : étendons l'**Exemple 1** en considérant le sujet *Sabrina* et l'objet o_2. D'après le *Tableau 10*, leurs niveaux de confidentialité sont comme suit : *csl(Sabrina, t_0) = 1* et *col(o_2, t_0) = 4*.

Supposons que *Bruno* a lu les objets o_1 et o_2 et *Sabrina* a lu l'objet o_2. Conformément aux ***Principes 2 et 3,*** le *niveau de confidentialité de Bruno* devient *plus élevé* que le *niveau de confidentialité de Sabrina*. Cela s'explique par le fait que le nombre d'objets lus par *Bruno* et ayant le niveau de confidentialité *4* (*2* objets) est supérieur au nombre d'objets ayant le niveau *4* lus par *Sabrina* (*1* objet). *4* étant le niveau de confidentialité le plus élevé.

Méthode 1 (motivée par les exemples *1* et *2*) :

Sur la base des définitions, des hypothèses et des principes présentés dans ce qui précède, nous proposons la méthode suivante pour évaluer le niveau de confidentialité d'un sujet :

1. Toujours appliquer le ***Principe 1***.
2. Appliquer le ***Principe 2*** lorsque des flux d'informations ont été reçus par le sujet.
3. Appliquer le ***Principe 3*** lorsque les niveaux de confidentialité des entités à partir desquelles des flux d'informations ont été reçus par le sujet, sont égaux.

Pour formaliser la *Méthode 1***,** nous définissons deux relations: $>_{mul}$ et $=_{mul}$ pour comparer les *multiensembles* selon *l'ordre lexicographique* [28]. En effet, l'application des ***Principes 1***, ***2*** et ***3*** nécessite l'utilisation d'un ordre de comparaison sur des multiensembles. **Exemple** : pour comparer les multiensembles *{4, 4, 5, 1}* et *{4,3, 2, 3, 1, 5}*, nous pouvons comparer lexicographiquement les séquences ordonnées *(5, 4, 4, 1)* et *(5, 4, 3, 3, 2, 1)*. Étant donné que *(5, 4, 4, 1)* est lexicographiquement supérieur à *(5, 4, 3, 3, 2, 1)*, il s'ensuit que $\{4, 4, 5, 1\} >_{mul} \{4, 3, 2, 3, 1, 5\}$. De même, $\{3, 3, 4, 0\} =_{mul} \{3, 4, 0, 3\}$.

D'après ce qui précède, nous constatons que nous pouvons comparer les niveaux de confidentialité de sujets, en fonction de leurs historiques d'accès en lecture, en utilisant la *Méthode 1*. Cette méthode peut être formalisée comme suit :

1. $csl(s, t) > csl(s', t)$ si $KnSL_c(s, t) >_{mul} KnSL_c(s', t)$
2. $csl(s, t) = csl(s', t)$ si $KnSL_c(s, t) =_{mul} KnSL_c(s', t)$

Tableau 11. Définition formelle de la Méthode 1

D'après la *Méthode 1*, à un instant *t* qui suit tous les accès cités dans les exemples *1* et *2*, nous obtenons le classement suivant des niveaux de confidentialité des sujets :
$csl(Bruno, t) > csl(Sabrina, t) > csl(Carl, t)$ étant donné que $KnSL_c(Bruno, t) = \{4, 4, 1\} >_{mul} KnSL_c(Sabrina, t) = \{4, 1\} >_{mul} KnSL_c(Carl, t) = \{2, 1\}$.

À noter que le ***Principe 3*** est satisfait car dans l'ordre lexicographique, si une séquence *A* est un préfixe propre d'une séquence *B*, alors $A < B$.

6.4.1.1 Considération de l'inférence pour l'évaluation des niveaux des sujets

Dans la section précédente, nous avons considéré les flux d'informations des objets vers les sujets pour évaluer les niveaux de confidentialité des sujets. Dans cette section, nous considérons les informations qui peuvent être déduites de l'historique des accès en lecture. Ce concept est connu dans la littérature sous le nom du problème d'inférence [31, 32, 33, 85]. Une inférence représente une faille de sécurité si des informations hautement classifiées peuvent être déduites à partir d'informations moins classifiées [85].

Nous distinguons deux types de problèmes d'inférences : l'agrégation d'informations et l'association d'informations.

Le problème d'*agrégation* d'informations se produit lorsque des informations de *même catégorie*, sont classées à un niveau de confidentialité plus élevé que chacun des niveaux associés aux informations considérées séparéments. **Exemple** : le contenu d'un dossier médical est *Secret*, mais l'information globale concernant l'ensemble des dossiers médicaux est *Top Secret*.

Le problème d'*association* d'informations, se produit lorsque deux ou plusieurs informations de *différentes catégories* sont classées à un niveau plus élevé que le niveau de chaque information, considérée séparément. **Exemple** : une liste comprenant des noms d'employés avec leurs fonctions est non classifiée. Une liste contenant les salaires correspondant aux fonctions est non classifiée. Cependant, la combinaison de ces deux listes a un niveau de confidentialité *Top secret*, puisqu'elle permet de connaître le salaire de chaque employé.

Nous définissons la fonction $Inf : 2^e \rightarrow L_c$ permettant d'attribuer un niveau de confidentialité aux informations inférées à partir d'un ensemble d'entités. Cette attribution de niveaux de confidentialité pourra, en général, être effectuée par des administrateurs de sécurité. **Exemple** : $Inf(\{o, o', o''\}) = 3$ signifie qu'une information *it* ayant un niveau de confidentialité *3* ($cil(it) = 3$) peut être inférée à partir des objets *o*, *o'* et *o''*.

Afin d'appliquer notre approche pour l'évaluation des niveaux de confidentialité des sujets, tout en considérant les cas où des informations hautement classifiées peuvent être inférées à partir d'informations moins classifiées, nous définissons les fonctions suivantes :

- *Inf_l$_c$: $2^e \rightarrow 2^{Lc}$* est une fonction qui associe à un ensemble d'entités, un multiensemble contenant les niveaux de confidentialité des informations qui peuvent être déduites à partir de ces entités. **Exemple** : *Inf_l$_c$(KnS(s, t)) = {4, 2}* signifie qu'à partir de l'ensemble d'entités *KnS(s, t)*, nous déduisons deux informations ayant des niveaux de confidentialité *4* et *2*.
- *KnSL$_c$A(s, t)* est l'union du multiensemble *KnSL$_c$(s, t)* et le multiensemble des niveaux d'informations déduites de *KnS(s, t)*. Plus formellement, *KnSL$_c$A(s, t) = KnSL$_c$(s, t) ∪ Inf_l$_c$(KnS(s, t))*.

Pour calculer *KnSL$_c$A(s, t)*, nous suivons les étapes ci-dessous :

1. Calculer *Inf_l$_c$(KnS(s, t))*.
2. Calculer *KnSL$_c$A(s, t)*.

Exemple : supposons que *Inf({o$_4$, o$_7$}) = 3*, *Inf({o$_6$, o$_7$}) = 4*, *KnS(Claude, t) = {Claude, o$_6$, o$_4$, o$_7$}*, *csl(Claude, t$_0$) = 2* et *KnSL$_c$(Claude, t) = {2, 1, 2, 1}*. Pour calculer *KnSL$_c$A(Claude, t)*, nous suivons ces étapes :

1. *Inf_l$_c$(KnS(Claude, t)) = {3, 4}*.
2. *KnSL$_c$A(Claude, t) = {2, 1, 2, 1, 3, 4}*.

Méthode 2

Nous pouvons ramener la comparaison des niveaux de confidentialité de deux sujets *s* et *s'* à la comparaison de *KnSL$_c$A(s, t)* et *KnSL$_c$A(s', t)*. Cette méthode peut être formalisée comme suit :

1. csl(s, t) > csl(s', t) si KnSL$_c$A(s, t) >$_{mul}$ KnSL$_c$A(s', t)
2. csl(s, t) = csl(s',t) si KnSL$_c$A(s, t) =$_{mul}$ KnSL$_c$A(s', t)

Tableau 12. Définition formelle de la Méthode 2

6.4.2 Évaluation des niveaux de confidentialité des objets

Les niveaux de confidentialité des objets sont évalués en considérant les informations contenues dans ces objets. Notons que les concepts introduits dans cette section seront très semblables à ceux développés dans la section précédente. Nous définissons *StSL$_c$(o, t')* qui

est le multiensemble des niveaux de confidentialité initiaux des entités *e* pour lesquelles il existe $t \leq t'$ et *St(o, e, t)* est vrai. **Exemple :** pour $col(o, t_0) = l_c$, $StSL_c(o, t) = \{l_c, l_c', l_c'\}$ signifie qu'à l'instant *t*, l'objet *o* de niveau initial l_c contient les informations de deux entités (sujets ou objets) différentes ayant respectivement comme niveau initial l_c'.

La définition de ce multiensemble nous permet d'évaluer les niveaux de confidentialité des objets, en fonction de l'historique des accès en écriture à ces objets. La méthode que nous développons est conçue pour satisfaire les principes suivants :

***Principe 4* :** le *niveau de confidentialité d'un objet* qui n'a pas reçu de flux d'informations d'autres entités, est défini par défaut. Ce niveau peut être déterminé par l'administrateur de sécurité.

***Principe 5* :** plus les *niveaux de confidentialité* des entités à partir desquelles un objet a reçu des flux d'informations augmente, plus *son niveau de confidentialité* augmente. Autrement dit, plus les niveaux de confidentialité initiaux des entités appartenant à *StS(o, t)* augmentent, plus *col(o, t)* augmente.

***Principe 6* :** plus le *nombre de flux d'informations* reçus par un objet, augmente, plus son *niveau de confidentialité* augmente. Autrement dit, plus le nombre d'entités appartenant à *StS(o, t)* augmente, plus *col(o, t)* augmente.

Ci-après, nous présentons des exemples pour motiver notre approche d'évaluation de niveaux de confidentialité des objets. Nous supposons que seuls les accès que nous présentons ont été réalisés. C'est-à-dire les niveaux des objets ne changent que sous l'effet de ces accès. Nous supposons également que les accès en écriture à l'origine des flux d'informations ont été effectués par des sujets distincts ayant le même niveau de confidentialité qui est égal à *1*.

Exemple 4 : considérons un premier cas où les informations de l'objet o_1 sont contenues dans l'objet o_5 et un second cas où les informations de l'objet o_4 sont contenues dans l'objet o_6. D'après le *Tableau 10*, nous avons ce qui suit : $col(o_1, t_0) = 4$, $col(o_4, t_0) = 2$, $col(o_5, t_0) = 1$ et $col(o_6, t_0) = 1$. Conformément au ***Principe 5***, le flux d'informations de o_1 vers o_5 rend le niveau de confidentialité de o_5 supérieur au niveau de confidentialité de o_6.

Cependant, ce principe n'est plus suffisant lorsque les niveaux de confidentialité des objets sont les mêmes.

Exemple 5 : étendons l'**Exemple 4** en considérant les objets o_2 et o_7 dont les niveaux de confidentialité sont donnés dans le *Tableau 10* comme suit : $col(o_7, t_0) = 1$ et $col(o_2, t_0) = 4$. Supposons que les informations des objets o_1 et o_2 sont contenues dans o_5 et les informations de o_2 sont contenues dans o_7. Conformément aux ***Principes 5*** et ***6,*** le niveau de confidentialité de o_5 sera plus élevé que le niveau de confidentialité de o_7.

Méthode 3 (à partir des exemples *4* et *5*)

L'évaluation des niveaux de confidentialité d'un objet peut être réalisée comme suit :

1. Toujours appliquer le ***Principe 4.***
2. Appliquer le ***Principe 5*** lorsque des flux d'informations ont été reçus par l'objet.
3. Appliquer le ***Principe 6*** lorsque les niveaux de confidentialité des entités à partir desquelles des flux d'informations ont été reçus par l'objet, sont égaux.

Cette méthode peut être formalisée comme suit :

1. $col(o, t) > col(o', t)$ *si* $StSL_c(o, t) >_{mul} StSL_c(o', t)$
2. $col(o, t) = col(o', t)$ *si* $StSL_c(o, t) =_{mul} StSL_c(o', t)$

Tableau 13. Définition formelle de la Méthode 3

D'après la *Méthode 3* et à un instant *t* qui suit tous les accès cités dans les exemples *4* et *5*, nous obtenons l'ordre suivant des niveaux de confidentialité des objets : $col(o_5, t) > col(o_7, t) > col(o_6, t)$ parce que $StSL_c(o_5, t) = \{4, 4, 1, 1\} >_{mul} StSL_c(o_7, t) = \{4, 1, 1\} >_{mul} StSL_c(o_6, t) = \{2, 1, 1\}$.

6.4.2.1 Considération de l'inférence pour l'évaluation des niveaux des objets

Afin d'appliquer notre approche pour l'évaluation des niveaux de confidentialité des objets et de considérer les cas où des informations hautement classifiées peuvent être inférées à partir des informations moins classifiées, nous définissons $StSL_cA(o, t)$ qui est l'union du multiensemble de niveaux $StSL_c(o, t)$ et le multiensemble des niveaux de confidentialité des informations qui peuvent être déduites de $StS(o, t)$. Plus formellement, $StSL_cA(o, t) = StSL_c(o, t) \cup Inf\_l_c(StS(o, t))$.

Exemple : supposons que $StS(o_3, t) = \{Carl, o_3, o_6, o_4, o_7\}$, $StSL_c(o_3, t) = \{1, 2, 1, 2, 1\}$, $Inf(\{o_4, o_7\}) = 3$, et $col(o_3, t_0) = 2$. Pour obtenir $StSL_cA(o_3, t)$, nous suivons les étapes suivantes :

1. $Inf\_l_c(StS(o_3, t)) = \{3\}$,
2. $StSL_cA(o_3, t) = StSL_c(o, t) \cup Inf\_l_c(StS(o_3, t)) = \{1, 2, 1, 2, 1, 3\}$.

Méthode 4

Nous pouvons comparer les niveaux de confidentialité de deux objets *o* et *o'* à un instant *t* en considérant les accès précédents et les informations qui peuvent en être déduites, en comparant $StSL_cA(o, t)$ avec $StSL_cA(o', t)$. Cette méthode peut être formalisée comme suit :

1. $col(o, t) > col(o', t)$ *si* $StSL_cA(o, t) >_{mul} StSL_cA(o', t)$
2. $col(o, t) = col(o', t)$ *si* $StSL_cA(o, t) =_{mul} StSL_cA(o', t)$

Tableau 14. Définition formelle de la Méthode 4

6.5 Évaluation des niveaux de confidentialité lors d'une requête d'accès

Dans la section précédente, nous avons formulé une approche qui permet de comparer les *niveaux de confidentialité des sujets* en fonction des informations qu'ils connaissent et les *niveaux de confidentialité des objets* en fonction des informations qu'ils contiennent. Dans cette section, nous présentons une adaptation de l'approche, présentée ci-haut, pour évaluer les *niveaux de confidentialité* des sujets et des objets lors d'une *requête d'accès*, tout en tenant compte des informations qui pourraient être inférées à partir de la combinaison des informations connues par le sujet demandeur d'accès et des informations contenues dans l'objet auquel l'accès est demandé.

6.5.1 Évaluation des niveaux de confidentialité des sujets lorsqu'un accès en écriture est demandé

Lorsqu'un sujet demande un accès en *écriture* à un objet, l'historique de ses accès est analysé pour déterminer si les informations contenues dans l'objet auquel l'accès est demandé, combinées avec les informations qu'il connaît, peuvent générer de nouvelles

informations [31, 32, 33, 85]. Si une inférence est possible alors la décision d'accès doit être prise en tenant compte d'un niveau de confidentialité du sujet recalculé. En effet, dans une situation pareille, un sujet serait capable de créer des informations qu'il ne connaît pas.

Exemple : considérons un cas où le sujet *Claude* a lu de l'objet o_4 à un instant *t* et demande d'accéder en écriture à l'objet o_5 à un instant ultérieur *t'*. D'après le *Tableau 10*, nous avons ce qui suit : $csl(Claude, t_0) = 2$, $col(o_5, t_0) = 1$, $col(o_4, t_0) = 2$. De plus, nous supposons que l'administrateur de sécurité a déterminé que $Inf(\{o_5, o_4\}) = 3$. Ainsi, l'accès de *Claude* en écriture à l'objet o_5 ayant le niveau de confidentialité *1*, permettrait d'avoir une information de niveau *3* dans o_5. Ceci s'explique par l'accès en lecture de *Claude* à un instant précédent à l'objet o_4 et que les informations contenues dans o_5 combinées aux informations contenues dans o_4 permettent d'avoir une information de niveau *3* ($Inf(\{o_5, o_4\}) = 3$). Pour cette raison, nous considérons que le niveau de confidentialité du sujet *Claude*, lors de cette demande d'accès, doit être supérieur à son niveau juste avant la demande d'accès puisque son accès créerait un flux d'informations du niveau *3* au niveau *1*.

La *Figure 27* représente les accès cités dans cet exemple. La colonne à gauche (*Instant t*) montre que le sujet Claude a lu l'objet o_4 *à l'instant t.* La colonne à droite (*Instant t'*) montre que le sujet *Claude*, représenté en pointillé, appartient à un niveau l_c qui est supérieur à son niveau lorsqu'il demande d'écrire dans o_5 à l'instant *t'*. Nous allons voir dans ce qui suit les principes que nous utilisons pour calculer les niveaux de confidentialité des sujets lorsqu'ils demandent des accès en écriture.

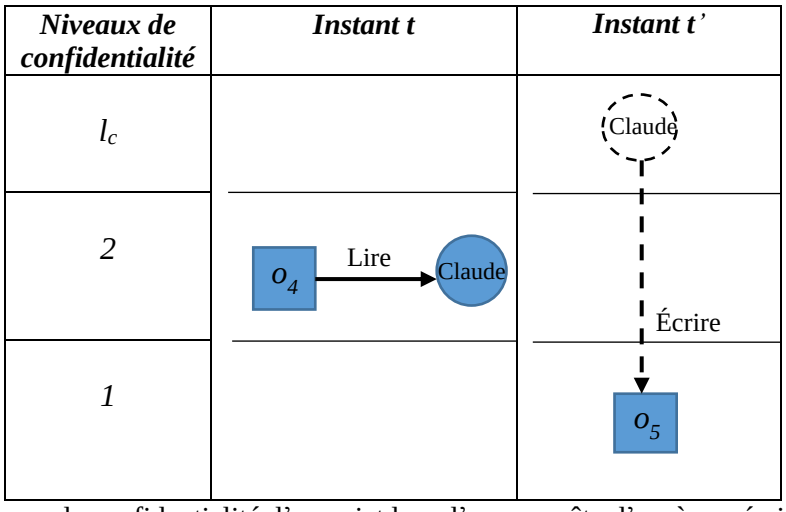


Figure 27. Niveau de confidentialité d'un sujet lors d'une requête d'accès en écriture

Afin d'appliquer notre approche, nous définissons les fonctions suivantes :

- *csol(s,o,t)* représente le niveau de confidentialité que doit avoir le sujet *s* quand il demande d'écrire dans un objet *o* à un instant *t*.
- *KnSS(s, o, t)* est l'union de l'ensemble des entités *e* dont les contenus sont connus par *s* à l'instant *t* et l'ensemble des entités *e'* qui ont transféré de l'information dans *o* jusqu'à l'instant *t*. Plus formellement, $KnSS(s, o, t) = \{e \mid Kn(s, e, t) = vrai\} \cup \{e' \mid St(o, e', t) = vrai\}$.
- $KnSSL_cA(s, o, t)$ est l'union du multiensemble des niveaux dans $KnSL_c(s, t)$ et du multiensemble des niveaux d'informations déduites de *KnSS(s, o, t)*. Plus formellement, $KnSSL_cA(s, o, t) = KnSL_c(s, t) \cup Inf\_l_c(KnSS(s, o, t))$.

Pour calculer $KnSSL_cA(s, o, t)$, nous suivons les étapes suivantes :

1. Calculer $KnSL_c(s, t)$.
2. Calculer *KnSS(s, o, t).*
3. Calculer $Inf\_l_c(KnSS(s, o, t))$ à partir de *KnSS(s, o, t).*
4. Calculer $KnSSL_cA(s, o, t) = KnSL_c(s, t) \cup Inf\_l_c(KnSS(s, o, t))$.

Exemple : supposons que *Claude* demande d'écrire dans o_3 à un instant *t*, avec $csl(Claude, t_0) = 2$, $col(o_3, t_0) = 2$, $KnS(Claude, t) = \{Claude, o_7, o_6, o_5\}$, $StS(o_3, t) = \{o_3, o_7, o_8\}$, et $Inf(\{o_8, o_6\}) = 3$. Les niveaux de confidentialité des autres objets sont définis dans le *Tableau 10*.

Pour déterminer $KnSSL_cA(Claude, o_3, t)$, nous suivons les étapes suivantes :

1. $KnSL_c(Claude, t) = \{2, 1, 1, 1\}$ (*Claude* connaît des informations contenues dans les objets o_7, o_6 *et* o_5 ayant chacun le niveau *1*, en plus de ses informations*).*
2. $KnSS(Claude, o_3, t) = \{Claude, o_3, o_7, o_8, o_6, o_5\}$ (l'union de l'ensemble d'entités connues par *Claude* et l'ensemble d'entités ayant des informations transférées dans o_3).
3. $Inf\_l_c(KnSS(Claude, o_3, t)) = 3$ (une information de niveau de confidentialité *3* peut être déduite à partir des informations contenues dans o_3 et des informations connues par *Claude* plus précisement de o_8 et o_6).

4. $KnSSL_cA(Claude, o_3, t) = \{2, 1, 1, 1, 3\}$ ($\{2, 1, 1, 1, 3\}$) est l'union du multiensemble des niveaux de confidentialité des entités ayant des informations connues par *Claude* et le singleton contenant le niveau de sécurité de l'information qui peut être déduite à partir des informations contenues dans o_3 et des informations connues par *Claude*).

Le multiensemble *{2,1,1,1,3}* permet de mettre en évidence le niveau de confidentialité de *Claude* dans le cadre de cette requête, après considération des flux d'information.

Méthode 5

D'après ce qui précède, nous pouvons comparer le niveau de confidentialité d'un sujet *s* demandant l'accès à un objet *o* au niveau de confidentialité d'un sujet *s'* demandant l'accès à un objet *o'*, en considérant les informations qui peuvent être inférées des informations connues par les sujet et des informations contenues dans les objets. Pour ce faire, nous comparons $KnSSL_cA(s, o, t)$ avec $KnSSL_cA(s', o', t)$. Cette méthode peut être formalisée comme suit :

1. $csol(s, o, t) > csol(s', o', t)$ si $KnSSL_cA(s, o, t) >_{mul} KnSSL_cA(s', o', t)$
2. $csol(s, o, t) = csol(s', o', t)$ si $KnSSL_cA(s, o, t) =_{mul} KnSSL_cA(s', o', t)$

Tableau 15. Définition formelle de la Méthode 5

6.5.2 Évaluation des niveaux de confidentialité des objets lorsqu'un accès en lecture est demandé

Dans cette section, nous considérons les informations qui peuvent être inférées à partir des infrmations connues par un sujet et des informations contenues dans l'objet auquel l'accès en lecture est demandé. Lorsqu'un sujet demande un accès en lecture à un objet, l'historique de ses accès est analysé pour déterminer si les informations contenues dans l'objet auquel l'accès est demandé, combinées avec les informations connues par le sujet, peuvent permettre d'inférer des informations ayant des niveaux de confidentialité plus élevés que le niveau de l'objet en question [31, 32, 33, 85]. Si une inférence est possible, le niveau de confidentialité de l'objet à utiliser pour déterminer la décision d'accès doit être recalculé en tenant compte de cette possibilité. En effet, dans une situation pareille, un

sujet serait capable de connaître des informations qui ont un niveau de confidentialité supérieur au niveau de l'objet lu.

Exemple : considérons un cas où le sujet *Carl* a lu l'objet o_5 à un instant *t* et demande d'accéder en lecture à l'objet o_4 à un instant ultérieur *t'*. D'après le *Tableau 10*, nous avons ce qui suit : $csl(Carl, t_0) = 1$, $col(o_5, t_0) = 1$, $col(o_4, t_0) = 2$. De plus, nous supposons que l'administrateur de sécurité a déterminé que $Inf(\{o_5, o_4\}) = 3$. Ainsi, l'accès de *Carl* à l'objet o_4 ayant le niveau de confidentialité *2* lui permettrait de connaître des informations de niveau *3* puisque *Carl* a accédé à un instant précédent à l'objet o_5 ayant le niveau *1* et les informations contenues dans o_5 combinées avec les informations contenues dans o_4 permettraient d'avoir une information de niveau 3 ($Inf(\{o_5, o_4\}) = 3$). Pour cette raison, nous considérons que le niveau de confidentialité de l'objet o_4 lors de cette demande d'accès doit être *supérieur à son niveau* puisque l'accès *de Carl* à o_4 lui permettrait de connaître une information ayant un niveau *3* même si le niveau de o_4 est *2*. Ceci créerait un flux d'informations du niveau *3* au niveau *1*.

La *Figure 28* représente les accès cités dans cet exemple. La colonne à gauche (*Instant t*) montre que le sujet *Carl* a lu l'objet o_5 à l'instant *t.* La colonne à droite (*Instant t'*) montre que le sujet *Carl* demande de lire l'objet o_4 représenté en pointillé et que o_4 appartient au niveau l_c qui est supérieur à son niveau lorsque le sujet *Carl* demande de le lire à l'instant *t'*. Nous allons voir dans ce qui suit les principes que nous utiliserons dans cette thèse pour calculer les niveaux de confidentialité lorsque des sujets demandent de les accéder en *lecture*.

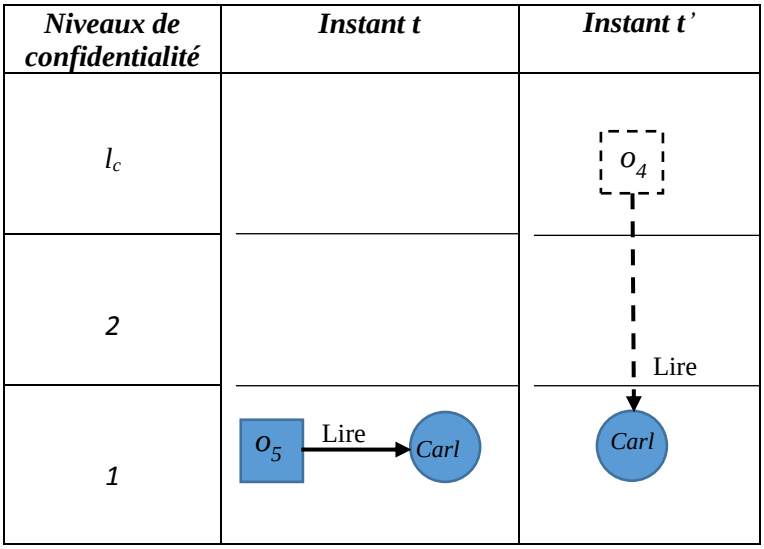


Figure 28. Niveau de confidentialité d'un objet lors d'une requête d'accès en lecture

Afin d'appliquer notre approche, nous définissons les fonctions suivantes :

- *cosl(o, s, t)* représente le niveau de confidentialité d'un objet lorsqu'un sujet *s* demande de le lire à un instant *t*.
- *StSS(s, o, t)* est l'union de l'ensemble des entités *e* pour lesquelles *Kn(s, e, t)* est vrai et l'ensemble des entités *e'* pour lesquelles *St(o, e', t)* est vrai. Plus formellement, $StSS(s, o, t) = \{e \mid Kn(s, e, t) = vrai\} \cup \{e' \mid St(o, e', t) = vrai\}$.
- $StSSL_cA(o, s, t)$ est l'union du multiensemble des niveaux dans $StSL_c(o, t)$ et du multiensemble des niveaux des informations qui peuvent être déduites de *StSS(o, s, t)*. Formellement, $StSSL_cA(o, s, t) = StSL_c(o, t) \cup Inf\_l_c(StSS(s, o, t))$.

Pour calculer $StSSL_cA(o, s, t)$, nous suivons les étapes suivantes :

1. Calculer $StSL_c(o, t)$,
2. Calculer *StSS(o, s , t)*,
3. Calculer $Inf\_l_c(StSS(o, s, t))$,
4. Calculer $StSSL_cA(o, s, t)$.

Exemple : supposons que *Claude* demande de lire o_3, avec $csl(Claude, t_0) = 2$, $col(o_3, t_0) = 2$, $KnS(Claude, t) = \{Claude, o_7, o_6, o_5\}$, $StS(o_3, t) = \{o_3, o_7, o_8\}$, et $Inf(\{o_8, o_6\}) = 3$.

Pour déterminer $StSSL_cA(o_3, Claude, t)$, nous suivons les étapes suivantes :

1. $StSL_c(o_3, t) = \{2, 1, 1\}$ (l'objet o_3 contient des informations provenant d'entités ayant les niveaux de sécurité *2, 1 et 1*).
2. $StSS(o_3, Claude, t) = \{Claude, o_3, o_8, o_7, o_6, o_5\}$ (l'union de l'ensemble d'entités ayant des informations contenues dans o_3 et l'ensemble d'entités ayant des informations connues par *Claude*).
3. $Inf\_l_c(StSS(o_3, Claude, t)) = 3$ (une information de niveau *3* peut être déduite à partir des informations contenues dans o_3 et connues par *Claude).*
4. $StSSL_cA(o_3, Claude, t) = \{2, 1, 1, 3\}$ (l'union du multiensemble des niveaux des entités ayant des informations contenues dans o_3 avec le niveau de l'information qui peut être déduite à partir des informations contenues dans o_3 et connues par *Claude* et plus précisément de o_8 et o_6).

Le multiensemble *{2, 1, 1, 3}* permet d'évaluer le niveau de confidentialité de o_3 dans le cas de cette requête, après considération des flux d'information.

Méthode 6

D'après ce qui précède, nous pouvons comparer les niveaux de deux objets *o* et *o'* en considérant les informations qui peuvent être déduites des informations connues par des sujets qui demandent de les lire et des informations contenues dans les objets auxquels l'accès est demandé. Pour ce faire, nous comparons $StSSL_cA(o, s, t)$ avec $StSSL_cA(o', s', t)$. Cette méthode peut être formalisée comme suit :

1. $cosl(o, s, t) > cosl(o', s', t)$ si $StSSL_cA(o, s, t) >_{mul} StSSL_cA(o', s', t)$
2. $cosl(o, s, t) = cosl(o', s', t)$ si $StSSL_cA(o, s, t) =_{mul} StSSL_cA(o', s', t)$

Tableau 16. Définition formelle de la Méthode 6

6.6 Considération des niveaux de confidentialité supérieurs aux niveaux de confidentialité initiaux des sujets et des objets

Dans cette section nous considérons des méthodes basées sur l'idée stipulant que les niveaux de confidentialité des sujets ou des objets n'augmentent que lorsqu'ils reçoivent des informations à partir d'entités ayant des niveaux de confidentialité supérieurs ou égaux aux niveaux de confidentialité initiaux des sujets et des objets.

6.6.1 Considération des niveaux de confidentialité supérieurs aux niveaux de confidentialité initiaux des sujets

Pour calculer les niveaux de confidentialité des sujets en considérant seulement les flux d'information reçus à partir des niveaux supérieurs ou égaux èa leurs niveaux de confidentialité initiaux, nous définissons les principes suivants :

***Principe 1b* :** le *niveau de confidentialité d'un sujet* qui n'a pas reçu de flux d'informations des niveaux *supérieurs ou égaux* à son niveau de confidentialité initial, est défini par défaut. Ce niveau peut être déterminé par l'administrateur de sécurité.

***Principe 2b* :** plus les *niveaux de confidentialité* des entités à partir desquelles un sujet a reçu des flux d'informations et ayant des niveaux de confidentialité *supérieurs ou égaux* à son niveau de confidentialité initial, augmente, plus le *niveau de confidentialité* de ce sujet augmente.

***Principe 3b* :** plus le *nombre de flux d'informations* reçus par un sujet à partir d'entités ayant des niveaux de confidentialité *supérieurs ou égaux* à son niveau de confidentialité initial augmente, plus le *niveau de confidentialité* de ce sujet augmente.

À partir des principes cités ci-dessus, nous définissons la *Méthode 1b* d'évaluation des niveaux de confidentialité des sujets qui consiste à suivre les étapes suivantes :

1. Toujours appliquer le ***Principe 1b***.
2. Appliquer le ***Principe 2b*** lorsque des flux d'informations ont été reçus par le sujet.
3. Appliquer le ***Principe 3b*** lorsque des flux d'informations ont été reçus par le sujet d'entités de même niveau de confidentialité.

Soit la définition suivante : pour tout $l_c \in KnSL_c(s, t)$, $KnSL_c^+(s, t)$ est le sous-multiensemble des éléments *de* $KnSL_c(s, t)$ ayant des valeurs *supérieures ou égales* à $csl(s, t_0)$. **Exemple** : Pour $csl(s, t_0) = l_c$, $KnSL_c^+(s, t) = \{l_c, l_c, l_c'\}$ signifie qu'à l'instant *t* le sujet *s* de niveau initial l_c connaît des informations provenants de deux entités ayant respectivement les niveaux initiaux l_c et l_c' et que $csl(s, t_0) \leq l_c$ et $csl(s, t_0) \leq l_c'$. La *Méthode 1b* peut être formalisée comme suit :

1. $csl(s, t) > csl(s', t)$ si $KnSL_c^+(s, t) >_{mul} KnSL_c^+(s', t)$
2. $csl(s, t) = csl(s', t)$ si $KnSL_c^+(s, t) =_{mul} KnSL_c^+(s', t)$

Tableau 17. Définition formelle de la Méthode 1b

Méthode 2b

Pour définir la *Méthode 2b*, nous définissons $KnSL_cA^+(s, t)$ qui est le sous-multiensemble *de* $KnSL_cA(s, t)$ ayant des valeurs supérieures ou égales à $csl(s, t_0)$. Plus formellement, $KnSL_cA^+(s, t) = \{l_c \in KnSL_cA(s, t) \mid l_c \geq csl(s, t_0)\}$.

Nous pouvons comparer les niveaux de confidentialité de deux sujets *s* et *s'* en considérant leurs accès précédents et les informations inférées de ces accès, en utilisant $KnSL_cA^+(s, t)$ et $KnSL_cA^+(s', t)$. La *Méthode 2b* peut être formalisée comme suit :

1. $csl(s, t) > csl(s', t)$ si $KnSL_cA^+(s, t) >_{mul} KnSL_cA^+(s', t)$
2. $csl(s, t) = csl(s', t)$ si $KnSL_cA^+(s, t) =_{mul} KnSL_cA^+(s', t)$

Tableau 18. Définition formelle de la Méthode 2b

6.6.2 Considération des niveaux de confidentialité supérieurs ou égaux aux niveaux initiaux de confidentialité des objets

Pour calculer les niveaux de confidentialité des objets en considérant seulement les flux d'informations reçus à partir des niveaux supérieurs ou égaux à leurs niveaux initiaux, nous définissons les principes suivants :

***Principe 4b* :** le *niveau de confidentialité d'un objet* qui n'a pas reçu de flux d'informations des niveaux *supérieurs ou égaux* à son niveau de confidentialité initial, est défini par défaut. Ce niveau peut être déterminé par l'administrateur de sécurité.

***Principe 5b* :** plus les *niveaux de confidentialité* des entités, à partir desquelles un objet a reçu des flux d'informations et ayant des niveaux de confidentialité *supérieurs ou égaux* à son niveau de confidentialité initial, augmente, plus le *niveau de confidentialité* de cet objet augmente.

***Principe 6b* :** plus le *nombre de flux d'informations* reçus par un objet à partir d'entités ayant des niveaux de confidentialité *supérieurs ou égaux* à son niveau de confidentialité initial, augmente, plus le *niveau de confidentialité* de cet objet augmente.

Méthode 3b

Pour présenter la *Méthode 3b,* nous définissons $StSL_c^+(o, t)$ qui est le sous-multiensemble des éléments de $StSL_c(o, t)$ et ayant des valeurs égales ou supérieures à $col(o, t_0)$. Plus formellement, $StSL_c^+(o, t) = \{l_c \in StSL_c(o, t) \mid l_c \geq col(o, t_0)\}$.

La *Méthode 3b* consiste à suivre les étapes suivantes :

1. Toujours appliquer le ***Principe 4b*.**
2. Appliquer le ***Principe 5b*** lorsque de nouveaux flux d'informations ont été reçus par l'objet.
3. Appliquer le ***Principe 6b*** lorsque des flux d'informations ont été reçus par l'objet à partir d'entités de même niveau de confidentialité.

La *Méthode 3b* peut être formalisée comme suit *:*

1. $col(o, t) > col(o', t)$ *si* $StSL_c^+(o, t) >_{mul} StSL_c^+(o', t)$
2. $col(o, t) = col(o', t)$ *si* $StSL_c^+(o, t) =_{mul} StSL_c^+(o', t)$

Tableau 19. Définition formelle de la Méthode 3b

Méthode 4b

Pour présenter la *Méthode 4b,* nous définissons $StSL_cA^+(o, t)$ qui est un sous-multiensemble des niveaux appartenant à $StSL_cA(o, t)$ et ayant des valeurs supérieures ou égales à $col(o, t_0)$. Plus formellement, $StSL_cA^+(o, t) = \{l_c \in StSL_cA(o, t) \mid l_c \geq col(o, t_0)\}$.

Nous pouvons comparer les niveaux de confidentialité de deux objets *o* et *o'* à un instant *t* en considérant les accès précédents et les informations qui peuvent en être déduites, en comparant $StSL_cA^+(o, t)$ avec $StSL_cA^+(o', t)$. La *Méthode 4b* est formalisée comme suit :

1. $col(o, t) > col(o', t)$ *si* $StSL_cA^+(o, t) >_{mul} StSL_cA^+(o', t)$
2. $col(o, t) = col(o', t)$ *si* $StSL_cA^+(o, t) =_{mul} StSL_cA^+(o', t)$

Tableau 20. Définition formelle de la Méthode 4b

6.6.3 Considération des niveaux de confidentialité supérieurs ou égaux aux niveaux initiaux de confidentialité des sujets et des objets lors d'une requête d'accès

Pour calculer les niveaux de confidentialité des sujets et des objets en considérant seulement les flux d'informations reçus à partir des niveaux supérieurs ou égaux à leurs niveaux de confidentialité initiaux, nous définissons la *Méthode 5b* pour le calcul des niveaux de confidentialité des sujets et la *Méthode 6b* pour le calcul des niveaux de confidentialité des objets.

Méthode 5b

Pour définir la *Méthode 5b*, nous définissons $KnSSL_cA^+(s, o, t)$ qui est le sous-multiensemble de $KnSSL_cA(s, o, t)$ ayant des valeurs supérieures ou égales à $csl(s, t_0)$. Plus formellement, $KnSSL_cA^+(s, t) = \{l_c \in KnSSL_cA(s, t) \mid l_c \geq csl(s, t_0)\}$.

Nous pouvons comparer le niveau de confidentialité d'un sujet *s* demandant l'accès à un objet *o*, au niveau de confidentialité d'un sujet *s'* demandant l'accès à un autre objet *o'*, en considérant les informations qui peuvent être inférées des informations connues par le sujet et des informations contenues dans l'objet. Pour ce faire, nous comparons $KnSSL_cA^+(s, o, t)$ avec $KnSSL_cA^+(s', o', t)$. Cette méthode peut être formalisée comme suit :

1. $csol(s, o, t) > csol(s', o', t)$ si $KnSSL_cA^+(s, o, t) >_{mul} KnSSL_cA^+(s', o', t)$
2. $csol(s, o, t) = csol(s', o', t)$ si $KnSSL_cA^+(s, o, t) =_{mul} KnSSL_cA^+(s', o', t)$

Tableau 21. Définition formelle de la Méthode 5b

Méthode 6b

Pour définir la *Méthode 6b*, nous définissons $StSSL_cA^+(o, s, t)$ qui est le sous-multiensemble de $StSSL_cA(s, o, t)$ ayant des valeurs égales ou supérieures à $col(o, t_0)$. Plus formellement, $StSSLcA^+(o, s, t) = \{l_c \in StSSL_cA(o, s, t) \mid l_c \geq col(o, t_0)\}$.

Nous pouvons comparer les niveaux de deux objets *o* et *o'* en considérant les informations qui peuvent être déduites des informations connues par des sujets qui demandent de les lire et des informations contenues dans les objets auxquels l'accès est

demandé. Pour ce faire, nous comparons $StSSL_cA^+(o, s, t)$ avec $StSSL_cA^+(o', s', t)$. Cette méthode peut être formalisée comme suit :

1. $cosl(o, s, t) > cosl(o', s', t)$ si $StSSL_cA^+(o, s, t) >_{mul} StSSL_cA^+(o', s', t)$
2. $cosl(o, s, t) = cosl(o', s', t)$ si $StSSL_cA^+(o, s, t) =_{mul} StSSL_cA^+(o', s', t)$

Tableau 22. Définition formelle de la Méthode 6b

6.7 Formules pour le calcul des niveaux de confidentialité

Dans la section précédente, nous avons défini les propriétés qui doivent être satisfaites dans notre approche pour l'évaluation des niveaux de confidentialité des sujets et des objets. Nous avons également discuté la construction d'un ordre de priorité sur ces niveaux. Toutefois, cet ordre de priorité offre seulement une comparaison qualitative. Par exemple, étant donné deux sujets *s* et *s'* ayant respectivement des niveaux de confidentialité *csl(s, t*) et *csl(s', t)*, un ordre de priorité sur ces niveaux sera utile afin de déterminer le sujet qui a le niveau de confidentialité le plus élevé. Des mesures quantitatives de ces niveaux peuvent être utiles et certaines méthodes de contrôle d'accès pourraient les exiger. Cependant, plusieurs formules qui respectent les principes de notre approche et qui mesurent quantitativement les niveaux de confidentialité, peuvent être développées. Dans cette section, nous proposons des formules pour le calcul des niveaux de confidentialité, nous décrivons leur construction, et nous prouvons leurs conformités par rapport aux principes que nous avons définis. Nous ajoutons le principe suivant :

***Principe 7* :** les valeurs des niveaux de confidentialité d'une entité *e* sont comprises entre une valeur minimale *min* et une valeur maximale *max*, où $min = cel(e, t_0)$ *et* $|L_c| \leq max < |L_c| + 1$.

6.7.1 Formule pour le calcul des niveaux de confidentialité des sujets

Tel que mentionné précédemment, les valeurs des niveaux de confidentialité des sujets augmentent avec le nombre et les niveaux de confidentialité des objets sources d'information. Dans cette section, nous présentons une formule qui permet de capturer ces principes.

Nous proposons de représenter le niveau de confidentialité d'un sujet *s* à un instant *t* (*csl(s, t)*) par un nombre décimal où sa partie entière représente le niveau de confidentialité le plus élevé à partir duquel des flux d'informations sont reçus et où la partie fractionnaire représente le nombre de flux de chaque niveau. Notons que nous soustrayons un flux à partir du nombre de flux ayant le niveau de confidentialité le plus élevé dans la partie fractionnaire parce que le flux est déjà représenté dans la partie entière.

Ci-dessous, la *Formule 1* que nous proposons pour calculer les niveaux de confidentialité des sujets.

$$csl(s, t) = Max(KnSL_cA(s, t)) + (\sum_{i=1}^{|Lc|} Num(i, (KnSL_cA(s, t) - \{Max(KnSL_cA(s, t))\})) \times 10^{-k\ ((|Lc|+1)-\ i)}$$

Tableau 23. Formule 1 : calcul des niveaux de confidentialité des sujets

Les composants de la *Formule 1* sont expliqués comme suit :

- $Max(KnSL_cA(s, t))$: le niveau de confidentialité maximum à partir duquel des informations sont transferées vers le sujet *s* jusqu'à l'instant *t*. *Max* retourne la valeur maximale dans un multiensemble de nombres entiers.
- $|L_c|$: le nombre de niveaux de confidentialité initiaux.
- *Num(i, M)* : le nombre d'occurrences de *i* dans le multiset *M*.
- 10^k : le nombre de flux d'informations à considérer.

Exemple : *5,23001*, où *k = 1*, représente le niveau de confidentialité d'un sujet obtenu par la *Formule 1* où $KnSL_cA(s, t) = \{5, 5, 5, 4, 4, 4, 1\}$ comme nous pouvons le voir dans la *Figure 29*. *5,23001* est obtenu de la façon suivante :

$5 +$

$2 \times 10^{-1\ ((5 + 1) - 5)} +$

$3 \times 10^{-1\ ((5 + 1) - 4)} +$

$0 \times 10^{-1\ ((5 + 1) - 3)} +$

$0 \times 10^{-1\ ((5 + 1) - 2)} +$

$1 \times 10^{-1\ ((5 + 1) - 1)}$

$= 5,23001$

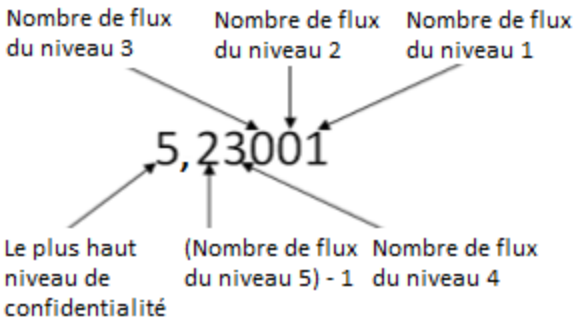


Figure 29. Calcul des niveaux de confidentialité

Exemple (Application de la formule) : considérons deux sujets *s* et *s'*. Le nombre de niveaux $|L_c|$ est égal à *5*. Le nombre maximum de flux d'informations à considérer est 10^2 *(k = 2). $KnSL_cA(s, t) = \{5,2,3,2\}$, $KnSL_cA(s', t) = \{5,4,3,3\}$.* Selon la *Méthode 2* (*Voir la section 6.4.1.1 de ce chapitre*), le niveau de confidentialité de *s'* doit être plus élevé que le niveau de confidentialité de *s* puisque chaque sujet a reçu des informations à partir du niveau *5* une fois alors que *s'* a reçu des informations du niveau *4* ce qui n'est pas le cas de *s*. Autrement dit, $KnSL_cA(s', t)$ est *lexicographiquement* supérieur *à* $KnSL_cA(s, t)$. Si nous appliquons la *Formule 1*, nous obtenons ce qui suit: *csl(s, t) = 5,00000102 (1)* et *csl(s', t) = 5,000102 (2)*. À partir de *(1)* et *(2)*, nous concluons que *csl(s', t) > csl (s, t)*.

Preuve de correction : cette section montre que la *Formule 1* pour le calcul des niveaux de confidentialité des sujets que nous avons proposée respecte les ***Principes 1***, ***2***, ***3*** et ***7***. Considérons un sujet qui n'a pas reçu de flux d'informations. Si nous appliquons notre formule le niveau de confidentialité sera égale à $Max(KnSL_cA(s, t))$ qui est la valeur minimale/initiale. Nous en déduisons que la *Formule 1* satisfait le ***Principe 1***.

Quand $Max(KnSL_cA(s, t))$ augmente, *csl(s, t)* augmente. En outre, lorsque *i* (niveau de confidentialité des entités) augmente, $10^{-k((|Lc|+1)- i)}$ augmente. Par conséquent *csl(s, t)* augmente. Ainsi, pour tout sujet *s*, *csl(s, t)* augmente à mesure que les niveaux de confidentialité des entités, à partir desquelles l'information est transférée à *s*, augmente. Nous en déduisons que la *Formule 1* satisfait le ***Principe 2***.

Lorsque $Num(i, (KnSL_cA(s, t) - \{Max(KnSL_cA(e,t))\})) \times 10^{-k((|Lc|+1)-i)}$ augmente, $\sum_{i=1}^{|Lc|} Num(i, (KnSL_cA(s, t) - \{Max(KnSL_cA(s, t))\})) \times 10^{-k\ ((|Lc|+1)- i)}$ augmente. Par conséquent, *csl(s, t)* augmente. Ainsi, pour tout sujet *s*, *csl(s, t)* augmente à mesure que le nombre de

différentes entités à partir desquelles des informations sont transférées à *s*, augmente. Nous en déduisons que la *Formule 1* satisfait le ***Principe 3***.

La valeur minimale qui pourrait être obtenue par cette formule est égale à $Max(KnSL_cA(s, t))$ lorsque $KnSL_cA(s, t) = csl(s, t_0)$. La valeur maximale qui pourrait être obtenue par cette formule ne peut pas être supérieure à $Max(KnSL_cA(s,t)) + 1$ et ne peut pas être inférieure à $|L_c|$. Par conséquent, les valeurs de niveaux de confidentialité sont entre la valeur minimale *min* et la valeur maximale *max*, où $min = csl(s, t_0)$, $max < |Lc| + 1$ et $max \geq |L_c|$. Cela satisfait le ***Principe 7***.

La *Formule 1* a été définie pour la *Méthode* 2. Cependant, elle est applicable dans le cas des méthodes *1*, 5, *1b*, *2b* et *5b*. En effet, pour obtenir les niveaux de confidentialité des sujets en considérant ces méthodes, il suffit de remplacer $KnSL_cA(s, t)$ dans la *Formule 1 par* $KnSL_c(s, t)$ pour la *Méthode 1, par* $KnSSL_cA(s, t)$ pour la *Méthode 5,* par $KnSL_c^+(s, t)$ pour la *Méthode 1b*, par $KnSL_cA^+(s, t)$ pour la *Méthode 2b* et par $KnSSL_cA^+(s, t)$ *pour la Méthode 5b (Voir la section 6.7.4).*

6.7.2 Formule pour le calcul des niveaux de confidentialité des objets

L'attribution des niveaux de confidentialité aux objets est similaire à l'attribution de ces niveaux aux sujets. Nous proposons de représenter le niveau de confidentialité des objets par un nombre décimal où la partie entière de $col(o, t)$ représente le niveau de confidentialité le plus élevé à partir duquel des informations sont reçues et où la partie fractionnaire représente le nombre de flux de chaque niveau.

Ci-dessous, la *Formule 2* qui considère la *Méthode 4* présentée dans la section *6.4.2.1* de ce chapitre :

$$col(o, t) = Max(StSL_cA(o, t)) + \left(\sum_{i=1}^{|Lc|} Num(i, (StSL_cA(o, t) - \{Max(StSL_cA(o, t))\}))\right) \times 10^{-k((|Lc|+1)-i)}$$

Tableau 24. Formule 2 : calcul des niveaux de confidentialité des objets

La preuve de cette formule est similaire à celle de l'attribution des niveaux de confidentialité aux sujets.

La *Formule 2* a été définie pour la *Méthode 4*. Cependant, elle est applicable dans le cas des *Méthodes 3, 6, 3b, 4b* et *6b*. En effet, pour obtenir les niveaux de confidentialité des

sujets en considérant ces méthodes, il suffit de remplacer $StSL_cA(s, t)$ dans la *Formule 2 par* $StSL_c(s, t)$ pour la *Méthode 3, par* $StSSL_cA(s, t)$ pour la *Méthode 6*, par $StSL_c^+(s, t)$ pour la *Méthode 3b*, par $StSL_cA^+(s, t)$ pour la *Méthode 4b* et par $StSSL_cA^+(s, t)$ *pour la Méthode 6b (Voir la section 6.7.4).*

6.7.3 Comportement des niveaux de confidentialité des sujets et des objets

Le graphique représenté dans la *Figure 30* est obtenu à partir des valeurs du *Tableau 25*, qui peuvent être obtenues à leur tour par les *Formules 1* et *2* lorsqu'appliquées pour les *Méthodes 1b*, *2b*, *3b*, *4b*, *5b* et *6b*. Les indices de *(1,1)* à *(1,9)* montrent que lorsqu'un sujet (ou un objet) n'a pas reçu de flux d'informations de niveaux de confidentialité supérieurs ou égaux à son niveau de confidentialité initial, la valeur du niveau de confidentialité de ce sujet (ou de cet objet) est égale à la valeur initiale par défaut, qui est égal à *2* dans cet exemple. Cela satisfait les ***Principes 1b*** et ***4b*.**

La partie gauche de la *Figure 30* montre qu'avec l'augmentation des niveaux de confidentialité des entités sources d'informations, le niveau de confidentialité du sujet (ou de l'objet) qui reçoit ces informations, augmente également. Cela satisfait les ***Principes 2b*** et ***5b***.

La partie gauche en haut de la *Figure 30* montre que lorsque les niveaux de confidentialité des entités sources d'informations, augmentent, le niveau de confidentialité du sujet (ou de l'objet) qui reçoit ces informations, augmente plus rapidement avec l'augmentation du nombre de ces entités. Cela satisfait les ***Principes 3b*** et ***6b***.

Les valeurs entre les indices *(1,1)* et *(5,9)* de la *Figure 30* montrent que, les valeurs de niveaux de confidentialité sont situés entre une valeur minimale *min* et une valeur maximale *max*, où dans cet exemple, $min = 2$ et $max \in [5, 6[$ où $5 = |L_c|$ et $6 = |L_c| + 1$. Cela satisfait le ***Principe 7***.

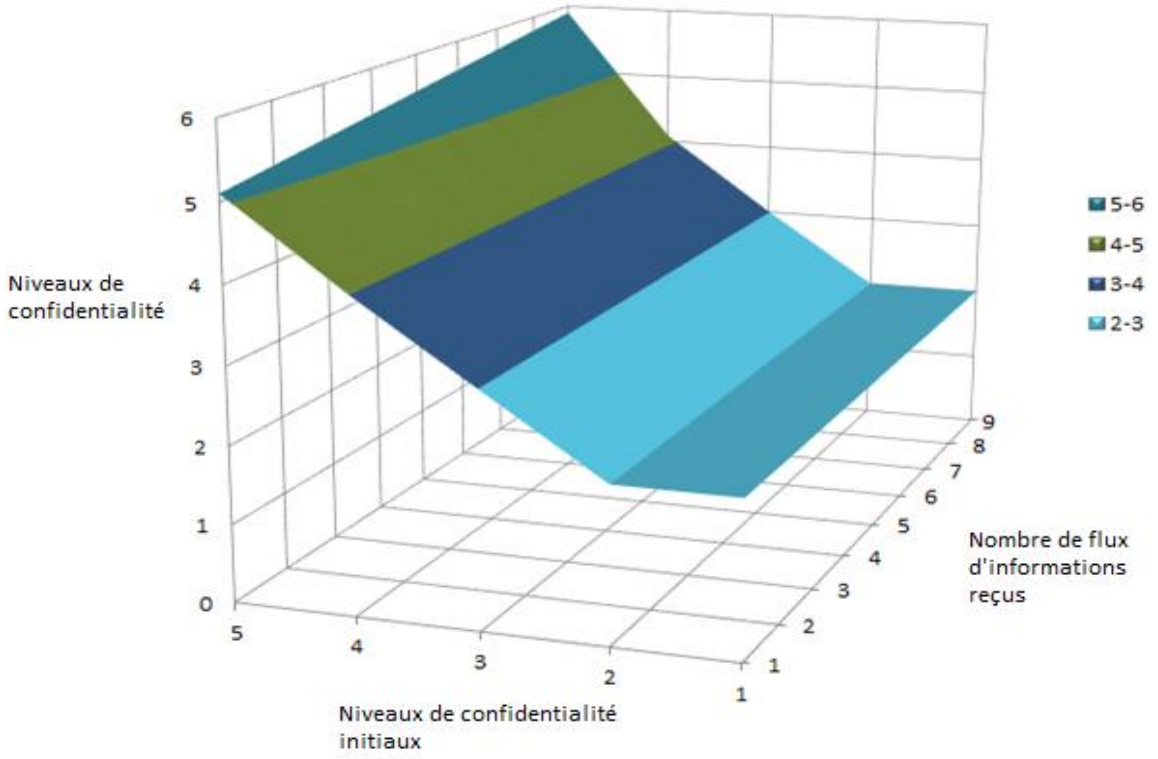


Figure 30. Comportement des niveaux de confidentialité

Niveaux de confidentialité / ***Nombre de flux d'informations***	*1*	*2*	*3*	*4*	*5*
9	*2*	*2,0009*	*3,0081*	*4,0801*	*5,8001*
8	*2*	*2,0008*	*3,0071*	*4,0701*	*5,7001*
7	*2*	*2,0007*	*3,0061*	*4,0601*	*5,6001*
6	*2*	*2,0006*	*3,0051*	*4,0501*	*5,5001*
5	*2*	*2,0005*	*3,0041*	*4,0401*	*5,4001*
4	*2*	*2,0004*	*3,0031*	*4,0301*	*5,3001*
3	*2*	*2,0003*	*3,0021*	*4,0201*	*5,2001*
2	*2*	*2,0002*	*3,0011*	*4,0101*	*5,1001*
1	*2*	*2,0001*	*3,0001*	*4,0001*	*5,0001*

Tableau 25. Comportement des niveaux de confidentialité

6.7.4 Formules pour le calcul des niveaux de confidentialité lorsqu'un accès est demandé

Tel que mentionné dans les sections *6.7.1* et *6.7.2* de ce chapitre, la *Formule 1* et la *Formule 2* peuvent être appliquées respectivenent pour la *Méthode 5* et la *Méthode 6.* Nous présentons la formule suivante pour le calcul des niveaux de confidentialité des sujets lorsqu'un accès en lecture est demandé (*Méthode 5*).

$$csol(s, o, t) = Max(KnSSL_cA(s, t)) + (\sum_{i=1}^{|Lc|} Num(i, (KnSSL_cA(s, t) - \{Max(KnSSL_cA(s, t))\})) \times 10^{-k\ ((|Lc|+1) - i)}$$

Tableau 26. Formule 3 : calcul des niveaux de confidentialité des sujets lorsqu'un accès en écriture est demandé

Exemple : l'exemple cité dans la section *6.5.1* donne le niveau de confidentialité suivant où $k = 1$: $csol(Claude, o_3, t) = 3{,}00013$.

Nous présentons également la formule suivante pour le calcul des niveaux de confidentialité des objets lorsqu'un accès en écriture est demandé (la *Méthode 6*).

$$cosl(o, s, t) = Max(StSSL_cA(o, t)) + (\sum_{i=1}^{|Lc|} Num(i, (StSSL_cA(o, t) - \{Max(StSSL_cA(o, t))\})) \times 10^{-k\ ((|Lc|+1) - i)}$$

Tableau 27. Formule 4 : calcul des niveaux de confidentialité des objets lorsqu'un accès en lecture est demandé

Exemple : l'exemple cité dans la section *6.5.2* donne le niveau de confidentialité suivant où $k = 1$: $cosl(o_3, Claude, t) = 3{,}0012$.

6.8 Calcul des niveaux d'intégrité basé sur les flux d'informations

Dans les sections précédentes, nous avons présenté une approche pour l'évaluation des niveaux de confidentialité des sujets et des objets. Cette approche est basée essentiellement sur l'idée stipulant que plus les niveaux de confidentialité des entités à partir desquels une entité reçoit des informations augmente, plus le niveau de cette entité augmente.

Dans cette section, nous allons présenter un ensemble de principes pour évaluer les niveaux d'intégrité. Une approche basée sur l'idée que les niveaux d'intégrité des sujets et des objets diminuent lorsque les sujets et les objets reçoivent des informations, pourrait être définie. Cette approche est duale à l'approche d'évaluation des niveaux de confidentialité des sujets et des objets présentée dans la section *6.4* de ce chapitre.

Cependant, nous allons nous contenter de présenter l'approche basée sur l'idée que les niveaux d'intégrité des sujets et des objets diminuent lorsque les sujets et les objets reçoivent des informations ayant des niveaux d'intégrité inférieurs ou égaux à leurs niveaux d'intégrité initiaux [12]. Le nombre d'entités ayant des niveaux d'intégrité inférieurs ou égaux à partir desquelles les informations sont reçues est un autre facteur à prendre en considération lors de l'évaluation des niveaux d'intégrité.

Pour évaluer les niveaux d'intégrité des entités, nous définissons la *Méthode 7* comme suit :

1. Pour les sujets et les objets qui n'ont pas reçu des flux d'informations à partir d'entités ayant des niveaux d'intégrité inférieurs ou égaux aux niveaux d'intégrité initiaux des sujets et des objets, appliquer le ***Principe 8*** qui stipule que le niveau d'intégrité est défini à une valeur initiale maximale qui peut être déterminée par l'administrateur de sécurité.
2. Toujours appliquer le ***Principe 9*** qui stipule que le niveau d'intégrité d'un sujet (ou d'un objet) diminue à mesure qu'il reçoit des flux d'informations à partir d'entités ayant des niveaux d'intégrité inférieurs ou égaux à son niveau d'intégrité initial.
3. À chaque fois que les niveaux d'intégrité des entités, à partir desquelles les flux d'informations sont transferées à un sujet (ou à un objet), sont identiques, appliquer le ***Principe 10*** qui stipule que le niveau d'intégrité d'un sujet (ou d'un objet) décroit lorsque le nombre d'entités, source des flux d'informations, ayant des niveaux d'intégrité inférieurs ou égaux à son niveau d'intégrité initial, croît.

6.8.1 Formule pour le calcul des niveaux d'intégrité des sujets

Les niveaux d'intégrité des sujets et des objets diminuent à mesure que le nombre d'entités, à partir desquelles les informations sont reçues augmente, et leurs niveaux d'intégrité diminuent. Par exemple, un sujet ou un objet qui a reçu des informations à partir d'un nombre élevé d'entités ayant des niveaux d'intégrité peu elevés aura un niveau d'intégrité inférieur au niveau d'intégrité d'un sujet ou d'un objet qui a reçu des informations à partir d'un nombre limité d'entités ayant des niveaux d'intégrité peu élevés. Dans cette section, nous présentons une formule qui respecte les principes de la *Méthode 7*. Cette formule peut

être utilisée pour calculer les niveaux d'intégrité de sujets (entités actives) ou des objets (entités passives).

Afin de calculer les niveaux d'intégrité des sujets, nous définissons ce qui suit :

- *isl (s, t)* représente le niveau d'intégrité d'un sujet *s* à un instant *t*. Ainsi, $isl(s, t_0)$ représente le niveau d'intégrité initial d'un sujet *s*.
- *iol(o, t)* représente le niveau d'intégrité d'un objet à un instant *t*. Ainsi, $iol(o, t_0)$ représente le niveau d'intégrité initiale d'un objet *o*.
- $KnSL_i(s, t)$ est le multiensemble des niveaux d'intégrité initiaux des entités *e* pour lesquelles *Kn(s, e, t)* est vrai.
- $KnSL_i^-(s, t)$ est le sous-multiensemble des niveaux d'intégrité appartenant à $KnSL_i(s, t)$ dont les éléments sont inférieurs ou égaux au niveau initial de *s*.
- $Min(KnSL_i^-(s, t))$ est le niveau d'intégrité minimal des entités à partir desquelles des informations sont transferées à *s* jusqu'à l'instant *t*. *Min* retourne la valeur minimale dans un multiensemble de nombres entiers.

Pour calculer les niveaux d'intégrité des sujets, nous définissons également le ***Principe 11*** qui stipule que les valeurs des niveaux d'intégrité d'un sujet *s* ou d'un objet *o* sont comprises entre une valeur maximale *max* et une valeur minimale *min*, où $max = isl(s, t_0)$ dans le cas des sujets, $max = isl(o, t_0)$ dans le cas des objets et $Min(L_i) - 1 < min \leq Min(L_i)$.

Le niveau d'intégrité est représenté par un nombre décimal où la partie entiére est fonction des niveaux d'intégrité (niveau d'intégrité le plus bas - 1) à partir desquels les informations sont reçues et où la partie fractionnaire est fonction du nombre de flux à partir de chaque niveau. Nous soustrayons de $10^k - 1$ (*9* dans l'exemple de la *Figure 31*) le nombre de flux de chaque niveau. Par exemple *0,76998* représente le niveau d'intégrité d'un sujet *s* où $KnSL_i^-(s, t) = \{1, 1, 1, 2, 2, 2, 5\}$ comme nous pouvons le voir dans la *Figure 31*. Notons que nous soustrayons un flux à partir du niveau d'intégrité le plus bas dans la partie fractionnaire parce que ce flux est représenté dans la partie entiére.

La *Formule 5* pour le calcul des niveaux d'intégrité des sujets est comme suit :

$$isl(s, t) = Min(KnSL_i^-(s, t)) - (\sum_{i=1}^{|Li|} Num(i, (KnSL_i^-(s, t) - \{Min(KnSL_i^-(s, t))\})) \times 10^{-k\,((|Li|+1)-\,i)}$$

Tableau 28. Formule 5 : calcul des niveaux d'intégrité des sujets

Dans l'exemple précédent, la valeur *0,76998, où k = 1*, est obtenue comme suit :

$1 -$

$2 \times 10^{-1\,((5+1)-5)} -$

$3 \times 10^{-1\,((5+1)-4)} -$

$0 \times 10^{-1\,((5+1)-3)} -$

$0 \times 10^{-1\,((5+1)-2)} -$

$1 \times 10^{-1\,((5+1)-1)}$

$= 0,76998$

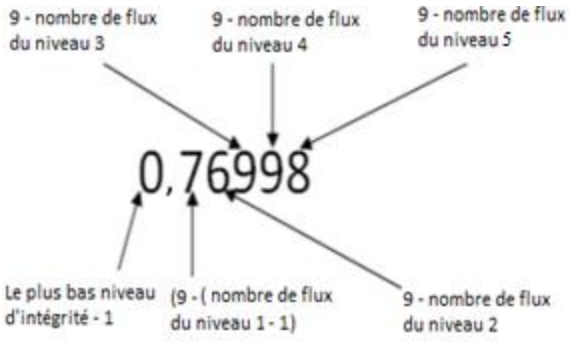


Figure 31. Calcul des niveaux d'intégrité

Preuve de correction : cette section montre que la formule pour l'évaluation de niveaux d'intégrité que nous avons proposé satisfait les ***Principes 8***, ***9***, ***10*** et ***11*** présentés précédemment. Lorsque nous appliquons notre formule à un sujet qui n'a pas d'historique de flux d'information reçus, le niveau d'intégrité sera égal à $Min(KnSL_i\,(s, t))$ qui est la valeur initiale maximale par défaut. Nous en déduisons que la *Formule 5* satisfait le ***Principe 8***.

Lorsque $Min(KnSL_i(s, t))$ diminue, $isl(s, t)$ diminue. En outre, lorsque i diminue, $10^{-k\,((|Li|+1)-i\,)}$ diminue. Par conséquent, $isl(s, t)$ diminue. Ainsi, pour tout sujet s, $isl(s, t)$ diminue

à mesure que les niveaux d'intégrité des entités, source des informations reçues par *s*, diminuent. Donc nous déduisons que la *Formule 5* satisfait le ***Principe 9***.

Lorsque $Num(i,(KnSL_i^-(s, t) - \{Min(KnSL_i^-(s, t))\}))$ augmente, $\sum_{i=1}^{|Li|} Num(i, (KnSL_i^-(s, t) - \{Min(KnSL_i^-(s, t))\})) \times 10^{-k((|Li|+1)-i)}$ diminue. Par conséquent $isl(s, t)$ diminue. Ainsi, pour tout sujet *s*, $isl(s, t)$ diminue à mesure que le nombre d'entités différentes, source des informations reçues par *s*, augmente. D'après ce qui précède, nous déduisons que la *Formule 5* satisfait le ***Principe 10***.

La valeur maximale qui pourrait être obtenue par cette formule est égale à $Min(KnSL_i^-(s, t))$ lorsque $KnSL_i^-(s, t)=csl(s, t)$. La valeur minimale pouvant être obtenue par cette formule ne peut pas être inférieure à $Min(KnSL_i^-(s, t)) - 1$ et ne peut excéder $Min(KnSL_i^-(s, t))$. Par conséquent, les valeurs des niveaux d'intégrité d'un sujet *s* sont entre une valeur maximale *max* et une valeur minimale *min*, où $max = isl(s, t_0)$ et $Min(L_i) - 1 < min \leq Min(L_i)$. Cela satisfait le ***Principe 11***.

6.8.2 Formule pour le calcul des niveaux d'intégrité des objets

Afin de calculer les niveaux d'intégrité des objets, nous définissons ce qui suit :

- $StSL_i(o, t)$ est le multiensemble de niveaux d'intégrité initiaux des entités *e* pour lesquels $St(o, e, t)$ est vrai.
- $StSL_i^-(o, t)$ est le sous-multiensemble des niveaux d'intégrité appartenant à $StSL_i(s, t)$ dont les éléments sont inférieurs ou égaux au niveau initial de *s*.
- $Min(StSL_i^-(o, t))$: le niveau d'intégrité minimal des entités à partir desquels des informations sont transferés à *o* jusqu'à l'instant *t*. *Min* retourne la valeur minimale dans un multiensemble de nombres entiers.

Nous proposons de représenter le niveau d'intégrité des objets par un nombre décimal où la partie entière représente le niveau d'intégrité le moins élevé à partir duquel des flux d'informations sont reçus et où la partie fractionnaire est fonction du nombre de flux de chaque niveau à partir duquel des flux sont reçus. Nous présentons la *Formule 6* pour le calcul des niveaux d'intégrité des objets comme suit :

$$iol(o,t) = Min(StSL_i^-(o,t)) - (\sum_{i=1}^{|Li|} Num(i, (StSL_i^-(o,t) - \{Min(StSL_i^-(o,t))\}))) \times 10^{-k((|Li|+1)-i)}$$

Tableau 29. Formule 6 : calcul des niveaux d'intégrité des objets

6.8.3 Comportement des niveaux d'intégrité des sujets et des objets

Le graphique représenté par la *Figure 32* est obtenu à partir des valeurs du *Tableau 30* qui peuvent être obtenues à leur tour par les *Formules 5* et *6*. Les indices de *(5,1)* à *(5,9)* dans la figure montrent que lorsqu'un sujet (ou un objet) n'a pas reçu de flux d'information de niveaux d'intégrité inférieurs ou égaux, la valeur de son niveau d'intégrité est égale à la valeur initiale par défaut, qui est égale à *4* dans cet exemple. Cela satisfait le ***Principe 8***.

Le côté droit de la figure montre qu'avec la diminution des niveaux d'intégrité des entités à partir desquelles les informations sont reçues, le niveau d'intégrité du sujet ou de l'objet qui reçoit ces informations, diminue également. Cela satisfait le ***Principe 9***.

Le côté droit en bas de la figure montre que lorsque les niveaux d'intégrité des entités sources d'informations, diminuent, le niveau d'intégrité du sujet (ou de l'objet) qui reçoit ces informations, diminue plus rapidement avec l'augmentation du nombre de ces entités. Cela satisfait le ***Principe 10***.

Les valeurs entre l'indice *(5,1)* et l'indice *(1,9)* de la figure montrent que, les valeurs de niveaux d'*intégrité* sont entre la valeur maximale *max* et la valeur minimale *min*, où dans cet exemple *max = 4* et *min = 0*. Cela satisfait le ***Principe 11***.

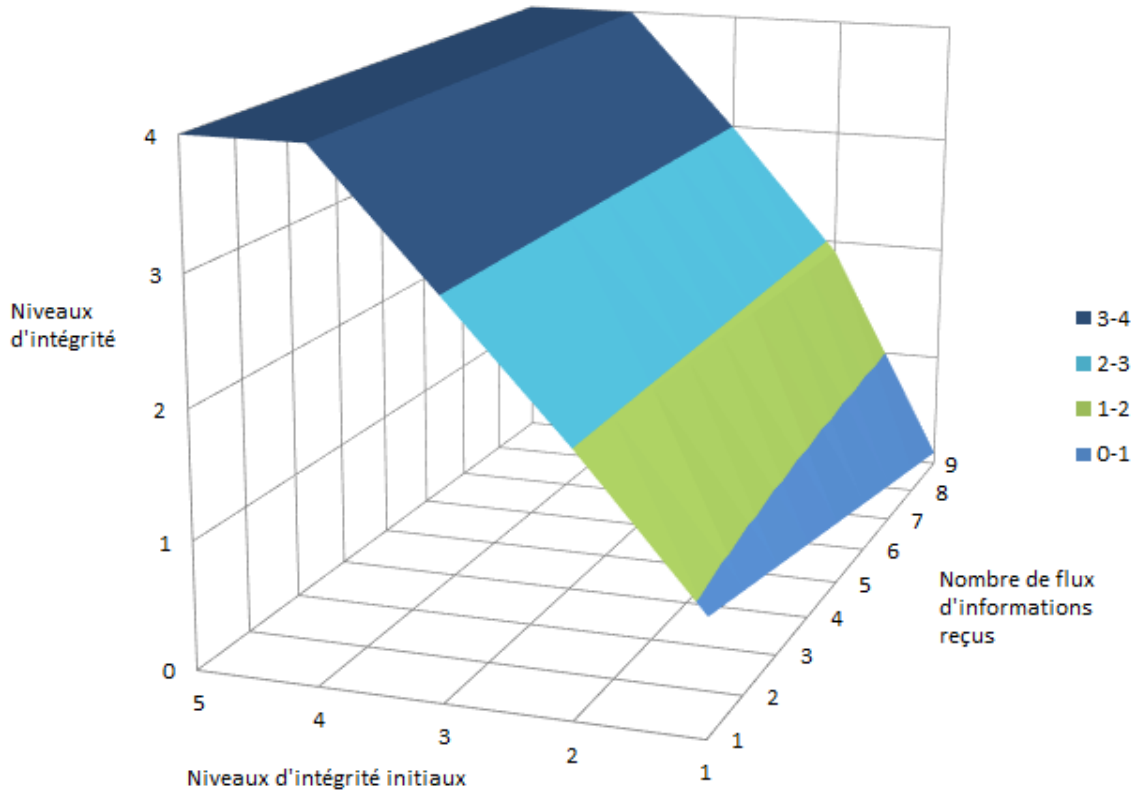


Figure 32. Comportement des niveaux d'intégrité

Niveaux d'intégrité / ***Nombre de flux d'informations***	*1*	*2*	*3*	*4*	*5*
9	*0,09999*	*1,90999*	*2,99099*	*3.99909*	*4*
8	*0,19999*	*1,91999*	*2,99199*	*3.99919*	*4*
7	*0,29999*	*1,92999*	*2.99299*	*3.99929*	*4*
6	*0,39999*	*1,93999*	*2.99399*	*3.99939*	*4*
5	*0,49999*	*1,94999*	*2.99499*	*3.99949*	*4*
4	*0,59999*	*1,95999*	*2.99599*	*3.99959*	*4*
3	*0,69999*	*1,96999*	*2.99699*	*3.99969*	*4*
2	*0,79999*	*1,97999*	*2.99799*	*3.99979*	*4*
1	*0,89999*	*1,98999*	*2.99899*	*3.99989*	*4*

Tableau 30. Comportement des niveaux d'intègrité

6.9 Modification du processus ABAC

Le contrôle d'accès basé sur les attributs (*ABAC*) [51] définit un paradigme de contrôle d'accès selon lequel les droits d'accès sont accordés aux utilisateurs par le biais de politiques basées sur des attributs liés aux sujets, aux objets, à l'environnement, etc. Ces attributs peuvent être comparés à des valeurs statiques ou à des valeurs dynamiques pour contrôler l'accès. Les niveaux de sécurité constituent un type particulier de ces attributs.

6.9.1 Mise à jour du processus de flux ABAC

Dans le processus de décision d'accès proposé dans le rapport décrivant le langage (*XACML*) [51], lorsque le point de décision de la politique (*PDP*) reçoit une requête d'accès, il demande des informations supplémentaires au point d'accès de la politique (*PAP*) et le point d'information de la politique (*PIP*) pour prendre une décision. La méthode que nous proposons ajoute de nouvelles étapes au cours desquelles, le service d'obligations envoie l'historique des accès au calculateur des niveaux de sécurité (étape *9*). Le processus de cette approche est illustré dans la *Figure 33*. C'est une modification du processus de la norme *ABAC* [51]. Les nouveaux composants et flux que nous avons ajoutés sont représentés en pointillés. Les étapes à suivre pour mettre à jour les niveaux de sécurité sont les suivantes :

1. Le *PEP* reçoit une demande d'accès (étape 1).
2. Le *PEP* transmet la demande d'accès au *PDP* (étape 2).
3. Le *PDP* consulte la politique de sécurité (étape 3).
4. Le *PDP* reçoit les attributs relatifs à la demande d'accès à partir du PIP (étapes *4*, *5* et *6*).
5. Le *PDP* détermine une décision d'accès à transmettre au *PEP* qui applique la décision d'accès (étape 7).
6. Une obligation est lancée (étape *8*).
7. Le service d'obligations envoie l'historique des accès au calculateur des niveaux de sécurité (étape *9*).

8. Le calculateur des niveaux de sécurité met à jour les attributs (niveaux de sécurité) des entités (sujets et objets) (étape *10*).

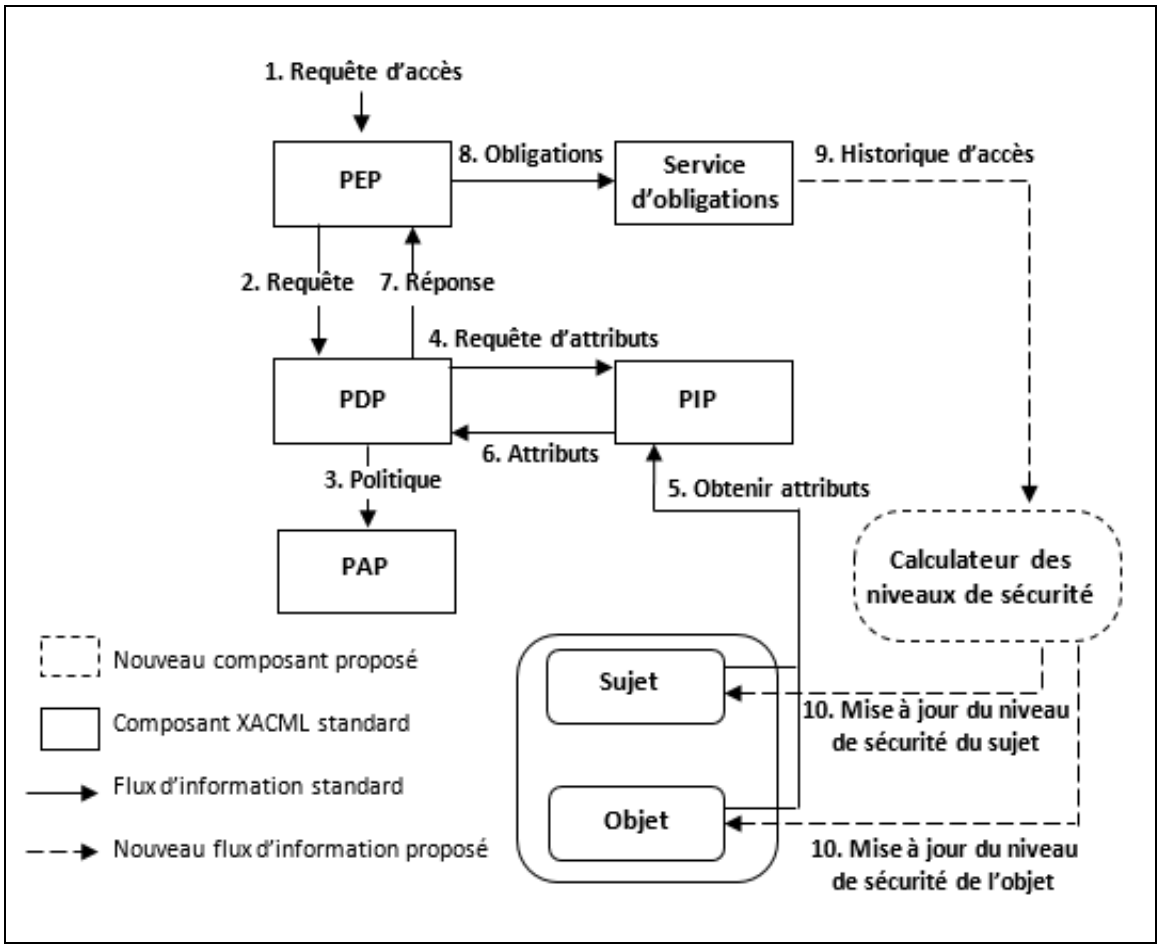


Figure 33. Processus proposé pour ABAC

Dans les deux sections suivantes, nous présentons deux cas d'utilisation de notre approche.

6.9.2 Cas d'utilisation 1

Considérons une table nommée *table1*, dans une base de données, contenant une liste de fonctions et de leurs salaires correspondants. Cette table a un niveau de confidentialité égal à *3*. Supposons que nous avons une politique de contrôle d'accès qui interdit le passage des informations à partir d'un niveau de confidentialité supérieur à un niveau inférieur. En outre, supposons que des informations sont ajoutées dans cette table par un processus *process1*, ayant un niveau de confidentialité égale à *3*, qui extrait des données d'une autre

table *table2* contenant une liste d'employés et leurs fonctions, et ayant un niveau de confidentialité *2*. Une inférence est possible à partir de *table1* et *table2* (*Inf (table1, table2) = 5*). En effet, la combinaison des informations contenues dans les deux tables mentionnées permettrait de connaître les salaires des employés qui représentent des renseignements personnels. Selon notre approche, une fois l'accès est accordé, le service d'obligations envoie l'historique des accès au calculateur de niveaux de sécurité qui met à jour l'attribut niveau de confidentialité de *table1*. Ainsi cet attribut sera égal à *5,001* lorsque $k = 1$.

Quand un processus *process2* ayant le niveau de confidentialité *5* demande de lire le contenu de *table1*, le *PDP* va consulter la politique de contrôle d'accès et recevoir les attributs liés à la demande d'accès du *PIP*. Ensuite, le *PDP* détermine une décision d'accès à appliquer par le *PEP*. Cette décision d'accès sera de refuser l'accès en lecture de *process2* à *table1* parce que si cette demande était accordée, l'information passerait d'un niveau élevé (*5,001*) à un niveau inférieur (*5*) ce qui est interdit par la politique de contrôle d'accès.

6.9.3 Cas d'utilisation 2

Considérons une table *table3*, dans une base de données, ayant un niveau d'intégrité *3*. Supposons que nous avons une politique de contrôle d'accès qui interdit le passage des informations vers des niveaux d'intégrité supérieurs. De plus, supposons que des informations sont ajoutées dans cette table par un processus *process3* ayant un niveau d'intégrité *2* dans le cadre d'une exception de durée limitée. Une fois l'accès est accordé, le service d'obligation envoie l'historique des accès au calculateur des niveaux de sécurité qui met à jour l'attribut du niveau d'intégrité de *table3*. Ainsi, cet attribut sera égal à *1,99899* lorsque $k = 1$.

Quand un processus *process4* ayant un niveau d'intégrité *2* demande de lire dans *table3*, le *PDP* va consulter la politique de contrôle d'accès et recevoir les attributs liés à la demande d'accès du *PIP*. Ensuite, le *PDP* détermine une décision d'accès qui doit être appliquée par le *PEP*. Cette décision d'accès sera de refuser l'accès de *process4* en lecture à *table3* parce que si cette demande était accordée, un flux d'information aurait eu lieu d'un niveau d'intégrité (*1,99899*) à un niveau d'intégrité plus élevé (*2*) ce qui est interdit par la politique de contrôle d'accès.

6.10 Tableau récapitulatif des notations de ce chapitre

Dans cette section, nous présentons le *Tableau 31* qui récapitule toutes les notations utilisées dans les sections précédentes de ce chapitre :

Notation	***Définition***
I	un ensemble d'informations.
S	un ensemble de sujets.
O	un ensemble d'objets.
T	un ensemble d'instants.
Kn(s, e, t)	le sujet *s* connaît le contenu de l'entité *e* à l'instant *t.*
St(o, e', t)	l'objet *o* contient les informations connues par ou contenues dans l'entité *e*, à l'instant *t.*
csl(s, t)	le niveau de confidentialité du sujet *s* à l'instant *t.*
$csl(s, t_0)$	le niveau de confidentialité initial du sujet *s*.
col(o, t)	le niveau de confidentialité de l'objet *o* à l'instant *t.*
$col(o, t_0)$	le niveau de confidentialité initial de l'objet *o.*
cel(e, t)	le niveau de confidentialité de l'entité *e* à l'instant *t.*
$cel(e, t_0)$	le niveau de confidentialité initial de l'entité *e.*
cil(it, t)	le niveau de confidentialité d'une information *it* à l'instant *t.*
isl(s, t)	le niveau d'intégrité du sujet *s* à l'instant *t.*
$isl(s, t_0)$	le niveau d'intégrité initial du sujet *s.*
iol(o, t)	le niveau d'intégrité de l'objet *o* à l'instant *t.*
$iol(o, t_0)$	le niveau d'intégrité initial de l'objet *o.*
iel(e, t)	le niveau d'intégrité de l'entité *e* à l'instant *t.*
$iel(e, t_0)$	le niveau d'intégrité initial de l'entité *e.*
KnS(s, t')	l'ensemble des entités *e* pour lesquelles *Kn(s, e, t)* est vrai.
StS(o, t')	l'ensemble des entités *e* pour lesquelles *St(o, e, t)* est vrai.
$KnSL_c(s, t)$	le multiensemble des niveaux de confidentialité des entités *e* pour lesquelles *Kn(s, e, t)* est vrai.
$KnSL_c^+(s, t)$	le sous-multiensemble des niveaux de confidentialité appartenant à $KnSL_c(s, t)$ dont les éléments sont supérieurs ou égaux au niveau initial de *s.*
$StSL_c(o, t)$	le multiensemble de niveaux de confidentialité d'entités *e* pour lesquelles *St(o, e, t)* est vrai.
$StSL_c^+(o, t)$	le sous-multiensemble des niveaux de confidentialité appartenant à *StSL(o, t)* dont les éléments sont supérieurs ou égaux au niveau initial de *o.*
$KnSL_i(s, t)$	le multiensemble des niveaux d'intégrité des *entités e* pour lesquelles *Kn(s, e, t)* est vrai.
$KnSL_i^-(s, t)$	le sous-multiensemble des niveaux d'intégrité appartenant à *KnSL(s, t)* dont ses éléments sont inférieurs ou égaux au niveau initial de *s.*
$StSL_i(o, t)$	le multiensemble de niveaux d'intégrité d'*entités e* pour lesquelles *St(o, e, t)* est vrai.
$StSL_i^-(o, t)$	le sous-multiensemble des niveaux d'intégrité appartenant à $StSL_c(o, t)$ dont les éléments sont inférieurs ou égaux au niveau initial de *o.*

$Inf(\{e_1,..,e_n\})$	le niveau de confidentialité d'une information qui peut être déduite à partir d'un ensemble d'entités.
$Inf\_l_c(o_1,..,o_n)$	le multiensemble des niveaux de confidentialité d'informations qui peuvent être déduites des informations contenues dans un ensemble d'objets et/ou connues par un ensemble de sujets .
$KnSL_cA(s, t)$	l'union des niveaux de confidentialité dans le multiensemble $KnSL_c(s, t)$ et le multiensemble des niveaux d'informations inférées de $KnS(s, t)$.
$KnSL_cA^+(s, t)$	le sous-multiensemble de $KnSL_cA(s, t)$ ayant des valeurs égales ou supérieures à $csl(s, t_0)$.
$StSL_cA(o, t)$	l'union du multiensemble de niveaux de confidentialité $StSL_c(o, t)$ et les niveaux de confidentialité d'informations qui peuvent être inférées de $StS(o, t)$.
$StSL_cA^+(o, t)$	le sous-multiensemble des niveaux de confidentialité appartenant à $StSL_cA(o, t)$ et ayant des valeurs égales ou supérieures à $col(o, t_0)$.
$cosl(o,s, t)$	le niveau de confidentialité d'un objet *o* lorsqu' un sujet *s* demande de le lire à un instant *t*.
$csol(s, o, t)$	le niveau de confidentialité d'un sujet *s* quand il demande d'écrire dans un objet *o* à un instant *t*.
$KnSS(s, o, t)$	l'union de l'ensemble des entités *e* pour lesquelles $Kn(s, e, t)$ est vrai et l'ensemble des entités *e'* pour lesquelles $St(o, e', t)$ est vrai, avec *e* différente de *e'*.
$KnSSL_cA(s, o, t)$	l'union du multiensemble des niveaux de confidentialité dans $KnSL_c(s, t)$ et le multiensemble des niveaux de confidentialité d'informations inférées de $KnSS(s, o, t)$.
$KnSSL_cA^+(s, o, t)$	le sous-multiensemble de $KnSSL_cA(s, o, t)$ ayant des valeurs égales ou supérieures à $csl(s, t_0)$.
$StSS(o, s, t)$	l'union de l'ensemble des entités *e* pour lesquelles $Kn(s, e, t)$ est vrai et l'ensemble des entités e' pour lesquelles $St(o, e'', t)$ est vrai, avec *e* est différente de *e''*.
$StSSL_cA(o, s, t)$	l'union du multiensemble des niveaux de confidentialité de $StSL_c(o, t)$ et le multiensemble des niveaux de confidentialité des informations qui peuvent être inférées de $StSS(o, s, t)$.
$StSSL_cA^+(o, s, t)$	le sous-multiensemble de $StSSL_cA(o, s, t)$ ayant des valeurs égales ou supérieures à $col(o, t_0)$.

Tableau 31. Tableau récapitulatif des notations

6.11 Discussion

Dans cette section, nous comparons notre travail à des travaux connexes et nous consacrons une section pour montrer la pertinence de notre approche en comparant l'évolution des niveaux de sécurité sous notre approche par rapport à d'autres modèles.

6.11.1 Travaux connexes

Le contrôle de flux d'informations est un sujet classique dans le domaine de la sécurité de l'information. Cependant, les méthodes qui proposent des techniques pour évaluer les niveaux de confidentialité ou d'intégrité des entités sur la base de flux d'informations et l'historique d'accès sont rares. Dans ce qui suit, nous présentons certains travaux connexes.

Le modèle *Bell-LaPadula (BLP)* [8] est basée sur un système de classifications et d'habilitations. Il interdit un flux d'informations d'un niveau de confidentialité supérieur à un niveau de confidentialité inférieur. Par exemple, un flux d'informations ne peut pas être créé à partir d'un niveau de confidentialité *Top Secret* vers le niveau de confidentialité *Classifié*.

Le modèle *Biba* [9] est un modèle avec des caractéristiques similaires, que nous avons également pris en considération. Ce modèle est basé sur des niveaux d'intégrité. Il interdit les flux d'un niveau inférieur à un niveau supérieur.

McLean [13] développe une théorie de flux d'informations. Cette théorie est utilisée pour développer un modèle de sécurité basé sur les flux.

Denning [27] étudie les mécanismes qui garantissent des flux d'informations sécurisés dans un système informatique. L'élément central de ce modèle est une structure de réseau justifiée par la sémantique des flux d'informations. Le modèle fournit une vue unificatrice de tous les systèmes qui limitent les flux d'informations et permet une classification en fonction des objectifs de sécurité.

Foley [40] décrit comment un modèle de sécurité multi-niveaux peut être utilisé pour mesurer le degré de confiance que l'on peut avoir à l'égard de la sécurité de la configuration d'un système.

Myers et *Liskov* [74] décrivent un modèle décentralisée d'étiquettes pour le contrôle des flux d'informations. Ce modèle améliore les modèles de sécurité multi-niveaux existants en permettant aux utilisateurs de déclassifier des informations d'une manière décentralisée et en améliorant le partage de données. Il prend en considération l'analyse statique des flux d'informations afin que les programmes soient certifiés qu'ils permettent seulement les

flux d'information acceptables. Nous croyons que chacun de ces modèles pourrait bénéficier de l'idée principale de notre approche qui propose un calcul des niveaux de confidentialité et d'intégrité des sujets et des objets.

La norme *FIPS 199* [37] présente des règles qui permettent d'évaluer les niveaux de sécurité des systèmes d'information pour les critères de confidentialité, d'intégrité et de disponibilité. Elle permet d'attribuer à chaque système une côte de sécurité (faible, modérée ou élevée pour chaque critère de sécurité). Le plus haut niveau devient le niveau de sécurité globale du système d'information. Notre approche considére les niveaux supérieurs de toutes les entités à partir desquelles des informations sont reçues.

La méthode la plus proche de la nôtre, dans le sens où elle utilise les flux d'informations résultant des accès passés pour évaluer les niveaux de confidentialité, est présentée dans [77] (*Voir la section 4.8 du chapitre 4*). Cette méthode utilise la logique floue pour affecter des degrés d'appartenance des sujets et des objets à chaque niveau de confidentialité selon des fonctions prédéfinies. Notons que notre méthode prend en compte les inférences possibles afin de déterminer les niveaux de sécurité, un aspect ignoré dans les modèles mentionnés ci-dessus. En outre, la méthode présentée dans [77] ne considère pas le critère d'intégrité.

6.11.2 Comparaison des comportements des niveaux de sécurité dans les modèles de sécurité

La *Figure 34* montre ce qui suit : sous le modèle *BL*P, le niveau de confidentialité (*2* dans notre cas) ne change pas comme nous pouvons le voir dans la *Figure 34(a)* parce que dans *BLP* les niveaux de confidentialité sont statiques et les flux à partir des niveaux de confidentialité supérieurs sont interdits. Cependant, la *Figure 34(b)*, montre que sous *HWM* lorsqu'un flux d'informations est crée à partir d'un niveau de confidentialité donné (*4* dans notre cas) à un niveau inférieur (*2* dans notre cas), le niveau de confidentialité supérieur est affecté au sujet ou à l'objet ayant un niveau de confidentialité inférieur et ce sera le niveau de confidentialité final du sujet ou de l'objet. La *Figure 34(c)* montre que dans notre approche même si un flux d'informations est créé à partir du niveau de confidentialité le plus élevé, le niveau de confidentialité continue à augmenter avec le nombre de flux

d'informations provenant d'entités différentes pour approcher la valeur $|L_c| + 1$ (*6* dans notre cas). La figure montre l'effet des flux répétés à partir du niveau de confidentilaité *5* qui conduit à une augmentation asymptotique du niveau de confidentilaité du sujet ou de l'objet vers le niveau *6*.

Sous le modèle *Biba*, le niveau d'intégrité (*4* dans notre cas) ne change pas comme nous pouvons le voir dans la *Figure 34(d)* parce que dans *Biba* les niveaux d'intégrité sont statiques et les flux à partir des niveaux d'intégrité inférieurs sont interdits. Cependant, la *Figure 34(e)*, montre que sous *LWM*, lorsqu'un flux d'informations est créée à partir d'un niveau d'intégrité inférieur (*2* dans notre cas) à un niveau d'intégrité plus élevé (*4* dans notre cas), le niveau d'intégrité inférieur est attribué au sujet ou à l'objet ayant le niveau d'intégrité élevé et il sera ainsi son niveau d'intégrité final (*2* dans notre cas). La *Figure 34(f)* montre que dans notre approche, malgré qu'un flux d'information est créée à partir du niveau d'intégrité le plus bas, le niveau d'intégrité continue à diminuer à mesure que le nombre de flux d'informations d'entités différentes augmente pour approcher la valeur $Min(L_i) - 1$ (*0* dans notre cas). La figure montre l'effet des flux répétés du niveau d'intégrité *1* qui conduit à une diminution asymptotique vers le niveau *0*.

D'aprés ces comparaisons, nous pouvons constater que notre approche d'attribution des niveaux de sécurité reflète mieux l'importance de l'intégrité et de la confidentialité des informations contenues dans les objets ou connues par le sujet.

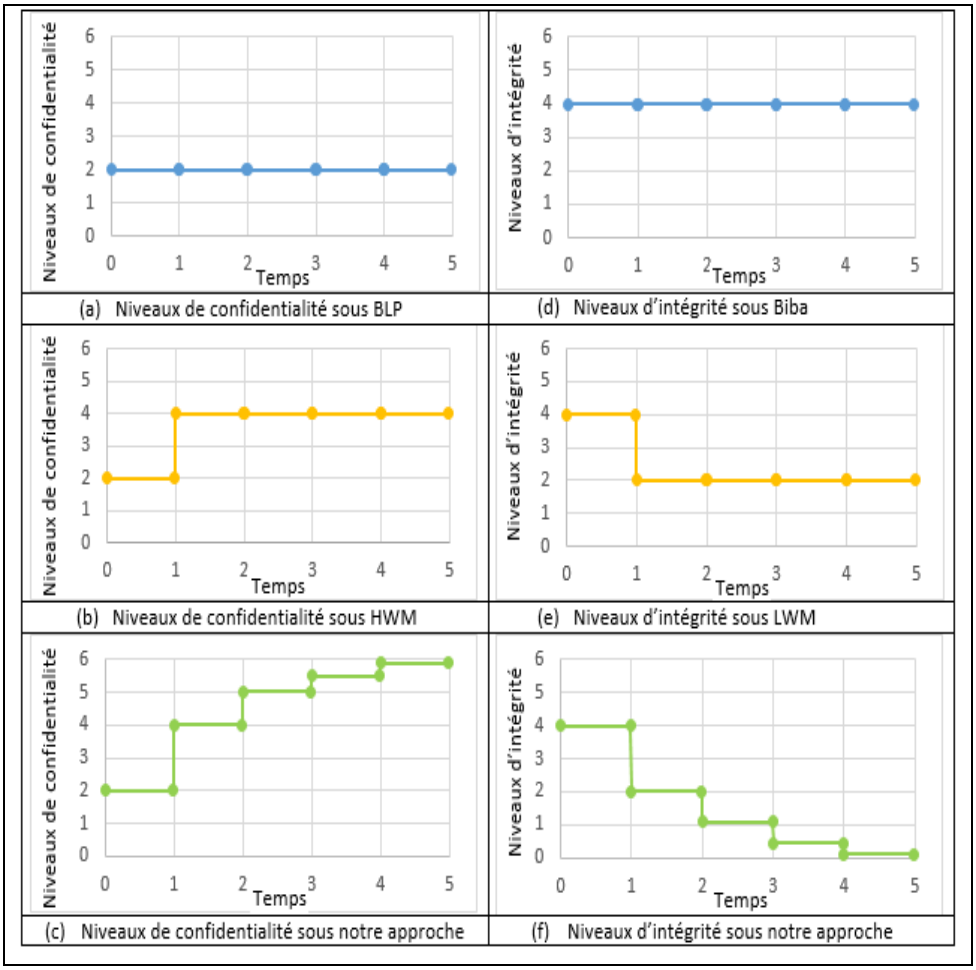


Figure 34. Comportement relatif aux niveaux de sécurité sous différents modèles

6.11.3 Mise à jour des niveaux

Il est à noter que notre approche permet la considération de la mise à jour des niveaux de sécurité. Cela pourrait être utile lorsque les entités sont déclassifiées. **Exemple :** Un appel d'offre après sa publication n'est plus confidentiel.

Cela est possible en mettant à jour les niveaux de sécurité dans les ensembles gardant la trace des flux d'informations reçus par les entités.

Soient :

- $KnSL_c e(s, t)$ l'ensemble des couples (entité e , niveaux de confidentialité l_c) tel que $Kn(s, e, t)$ est vrai.

- La fonction $MAJ\_l_c(e, t') = l_c'$ qui permet de mettre à jour le niveau de confidentialité de l'entité e pour qu'il soit égale à l_c'.

Exemple :

Si $KnSL_ce(s, t) = \{(o_1,5),(o_2,5), (o_3,5)\}$, en suivant les mêmes principes des formules présentées dans cette thèse, nous obtenons un niveau de confidentialité du sujet *s* à l'instant *t* égale à *5,2*. L'application d'une fonction $MAJ\_l_c(o_3, t'') = 1$ nous donne $KnSL_ce(s, t'') = \{(o_1,5),(o_2,5), (o_3,1)\}$. Le niveau de confidentialité du sujet *s* à l'instant *t''* devient alors égal à *5,10001*.

6.12 Conclusion

La principale contribution de ce chapitre est une approche fondée sur les flux d'informations pour l'évaluation des niveaux de sécurité des sujets et des objets. Cette approche est basée sur l'historique des flux d'informations, ainsi que les informations qui peuvent en être inferées (agrégation et association de l'information) dans le cas de la confidentialité.

Nous avons présenté plusieurs exemples qui justifient notre approche en termes intuitifs. Nous avons également présenté des définitions formelles de notre approche et des formules pour quantifier les niveaux de confidentialité et d'intégrité. À notre connaissance, notre travail représente une des rares tentatives, dans la littérature, pour élaborer une approche fondée sur le flux d'informations pour l'évaluation des niveaux de sécurité. Nous avons montré que notre approche permet une évaluation plus précise que les méthodes précédemment connues des modèles du *plus haut* et du *plus bas niveau*. Cette approche peut être utilisée dans les environnements web et infonuagiques où les flux d'informations sont en constante évolution, étant donné que notre méthode peut être invoquée dynamiquement lorsque les informations sont transferées entre les sujets et les objets.

Notons que notre approche est basée sur une attribution a priori des niveaux de sécurité des sujets et des objets. Cela signifie qu'elle ne couvre pas d'autres paramètres socio-techniques qui pourraient être prises en considération pour refléter la réalité de la confiance

placée sur des sujets tels que le comportement des utilisateurs, la collusion avec d'autres utilisateurs, etc.

Dans le chapitre suivant nous présentons notre approche basée sur les niveaux de sécurité les sujets et des objets pour le calcul de la potentialité de la menace des requêtes d'accès.

Chapitre 7 : Calcul de la potentialité de la menace des demandes d'accès

7.1 Introduction

Dans ce chapitre, nous proposons une approche pour le calcul de la *potentialité de la menace* qui représente la possibilité de l'occurrence du risque. Le calcul de la *potentialité de la menace* passe par le calcul de la *potentialité intrinsèque* qui est une évaluation maximaliste de la possibilité de l'occurrence du risque, sans la considération des mesures de sécurité [23]. Ainsi, la potentialité *de la menace* dans notre approche peut être décrite comme suit : *Potentialité de la menace = Potentialité de la menace intrinsèque – Valeur de la réduction de la potentialité de la menace.*

Les modèles des menaces internes dans la littérature distinguent les éléments suivants : la *capacité des utilisateurs*, la *motivation* et l'*opportunité* (*modèle CMO*) [86, 99-101].

Dans notre approche, la *capacité des utilisateurs* ne sera pas considérée pour le calcul de la *potentialité de la menace* des requêtes d'accès parce que la portée de notre approche inclut seulement les risques censés provenir des activités ordinaires des employés et non des attaques sophistiquées [7] .

La première dimension dont nous tenons compte pour le calcul de la *potentialité intrinsèque de la menace*, est la *motivation*. Selon *Cappelli* et *al.* [17], les employés internes à l'origine des menaces occupent généralement des positions en bas de la hiérarchie des entreprises. Pour cela, nous faisons l'hypothèse que la *motivation* pour violer la politique de sécurité *augmente* lorsque le niveau de fiabilité des employés *diminue*.

La deuxième dimension que nous considérons pour le calcul de la *potentialité intrinsèque de la menace*, est l'*opportunité* qui est causée par l'importance du privilège accordé lors d'une dérogation. Cela plaide en faveur de l'idée présentée dans [4] : « une opportunité fait un voleur ». Pour cela, nous faisons l'hypothèse que l'*opportunité augmente* lorsque la sensibilité de l'objet à accéder *augmente*.

D’après ce qui précède, nous faisons une hypothèse générale qui considère que la *potentialité intrinsèque de la menace* dépend de l’importance des flux d’informations entre les niveaux de sécurité des objets et les niveaux de sécurité des sujets. Autrement dit, nous supposons une *corrélation* entre le flux d’information qui peut résulter d’un accès permis et la *potentialité intrinsèque de la menace*.

Nous considérons que la *potentialité intrinsèque de la menace sur la confidentialité* augmente lorsque l’information peut passer à des niveaux de confidentialité moins élevés, et elle diminue lorsque l’information peut passer à des niveaux de confidentialité plus élevés. Cela s’explique par le fait que le passage de l’information vers le bas augmente la possibilité de sa divulgation à des sujets non fiables. De même la *potentialité intrinsèque de la menace sur l’intégrité* augmente lorsque l’information peut passer à des niveaux d’intégrité plus élevés, et elle diminue lorsque l’information peut passer à des niveaux d’intégrité moins élevés. Cela s’explique par le fait que le passage de l’information vers le haut augmente la possibilité de la dégradation de l’intégrité des informations aux niveaux élevés à cause de l’information ayant un niveau d’intégrité bas.

La valeur de la *potentialité intrinsèque de la menace* obtenue sera utilisée pour calculer la *potentialité de la menace.* À cet effet, nous adoptons des concepts de la méthodologie *Méhari* [23] pour intégrer l’évaluation de l’effet des mesures de sécurité permettant la réduction de *potentialité de la menace* (mesures structurelles, mesures dissuasives et mesures préventives).

Notre approche pour le calcul de la *potentialité de la menace* considère les facteurs suivants :

- L’*objectif de sécurité* visé (confidentialité ou intégrité).
- L’*action demandée* (lecture ou écriture).
- La *motivation* qui peut être déduite à partir des *caractéristiques personnelles* des utilisateurs permettant d’évaluer à quel point un groupe d’employés est fiable ou à quel point il peut être motivé à concrétiser la menace. Dans notre approche, ce facteur sera représenté par le *niveau de confidentialité* ou le *niveau d’intégrité* du sujet demandeur d’accès.

- L'*opportunité* qui représente la tentation causée par l'attribution du nouveau privilège. Dans notre approche, ce facteur sera représenté par le *niveau de confidentialité* ou le *niveau d'intégrité* de l'objet à accéder.
- Les *mesures de sécurité réductrices de la potentialité de la menace*.

Ce chapitre est organisé de la façon suivante : la section *2* décrit notre approche pour le calcul de la *potentialité intrinsèque de la menace* lorsque l'objectif de *confidentialité* est visé. Dans la section *3*, nous décrivons notre approche pour le calcul de la *potentialité intrinsèque de la menace* lorsque l'objectif d'*intégrité* est visé. Dans la section *4*, nous présentons des formules pour le calcul de la *potentialité intrinsèque de la menace* et des formules pour le calcul de la *potentialité de la menace*. Dans la section *5*, nous présentons les travaux connexes à notre travail et nous discutons les limites de notre approche. Nous concluons ce chapitre dans la section *6* par discuter les contributions présentées et leur utilisation dans cette thèse.

7.2 Approche pour le calcul de la potentialité intrinsèque de la menace lorsque la confidentialité est visée

Dans cette section, nous expliquons les fondements conceptuels de notre approche de calcul de la *potentialité intrinsèque de la menace* lorsque l'objectif de confidentialité est visé.

7.2.1 Hypothèses

Rappelons les fonctions d'attribution des niveaux de confidentialité présentées dans le chapitre *6* :

- *csl(s, t)* représente le niveau de confidentialité d'un sujet *s* à un instant *t*.
- *col(o, t)* représente le niveau de confidentialité d'un objet *o* à un instant *t*.

Notre approche fait la distinction entre des demandes d'accès qui sont acceptées par défaut et les demandes d'accès où les décisions d'accès dépendent de la valeur calculée du risque.

7.2.1.1 Accès acceptés par défaut

Si *csl(s, t)* ≥ *col(o, t)* alors toutes les demandes d'accès en *lecture* à un instant *t*, par un sujet *s* à un objet *o*, seront autorisées.

Si *csl(s, t)* ≤ *col(o, t)* alors toutes les demandes d'accès en *écriture* à un instant *t*, par un sujet *s* à un objet *o*, seront autorisées.

7.2.1.2 Accès basés sur le risque

Si *csl(s, t)* < *col(o, t)* alors une requête d'accès en *lecture* à un instant *t*, par un sujet *s* à un objet *o*, ne sera autorisée que si le risque qui lui est associé est inférieur au seuil du risque acceptable spécifié.

Si *csl(s, t)* > *col(o, t)* alors une requête d'accès en *écriture* à un instant *t*, par un sujet *s* à un objet *o*, ne sera autorisée que si le risque qui lui est associé est inférieur au seuil de risque acceptable spécifié.

Nous considérons que la *potentialité intrinsèque de la menace* dans un système de contrôle d'accès, où la confidentialité est visée, peut être vue comme la potentialité intrinsèque de la divulgation des informations contenues dans un objet donné. Nous considérons que la *potentialité intrinsèque* est fonction du niveau de confidentialité du sujet qui indique son niveau de fiabilité, et le niveau de confidentialité de l'objet qui représente l'importance de l'opportunité. Par exemple, la *potentialité intrinsèque de la menace* devrait être très élevée dans le cas d'une personne, ayant un niveau de confidentialité *Non classé*, qui a accès en *lecture* à des informations *très secrètes* mais relativement plus faible si le même accès est accordé à une personne qui a un niveau de confidentialité *Secret*.

La *Figure 35* représente l'approche de calcul de la *potentialité intrinsèque de la menace*.

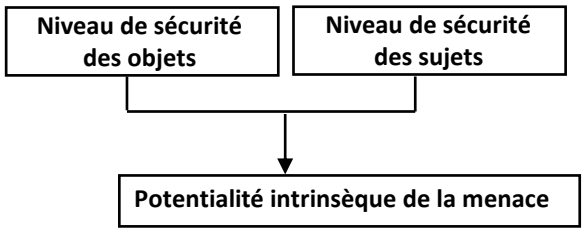


Figure 35. Calcul de la potentialité intrinsèque de la menace

7.2.2 Principes pour le calcul de la potentialité intrinsèque de la menace sur la confidentialité

Pour évaluer la *potentialité intrinsèque de la menace*, nous utilisons l'intuition derrière le modèle *Bell-LaPadula* dont les règles obligatoires préviennent le flux d'informations d'un haut niveau de confidentialité à un niveau de confidentialité plus bas. Le modèle *Bell-LaPadula* a une vision binaire de la potentialité de la menace [20]. Dans le cas des accès en lecture, la *potentialité intrinsèque de la menace* est nulle si c*ol(o, t)* $\leq$ *csl(s, t)* et elle est égale à *1* autrement. L'inverse est vrai dans le cas des accès en écriture, c'est-à-dire une *potentialité intrinsèque* de *1* si *csl(s, t)* $>$ *col(o, t)* et nulle autrement.

Dans notre approche, nous adoptons les principes suivants :

- ***Principe 12* :** la *potentialité intrinsèque de la menace* sur *la confidentialité* est *non nulle* si un sujet *s* demande d'accéder en *lecture*, à un instant *t*, à un objet *o*, tel que *csl(s, t) < col(o, t)*. En d'autre termes, si *csl(s, t)* $\geq$ *col(o, t)*, pour toute demande faite à un instant *t*, par un sujet *s* pour accéder en *lecture* à un objet *o*, la *potentialité intrinsèque de la menace* est *nulle*.
- ***Principe 13* :** la *potentialité intrinsèque de la menace* sur *la confidentialité* est *non nulle* si un sujet *s* demande d'accéder en *écriture*, à un instant *t*, à un objet *o*, tel que *csl(s, t) > col(o, t)*. En d'autre termes, si *csl(s, t)* $\leq$ *col(o, t)*, pour toute demande faite à un instant *t* par un sujet *s* pour accéder en écriture à un objet *o*, la *potentialité intrinsèque de la menace* est *nulle*.

Au lieu d'adopter la vision binaire du modèle *Bell-LaPadula* pour évaluer la *potentialité intrinsèque de la menace* pour la confidentialité des accès en *lecture*, nous proposons de considérer les principes suivants qui remplacent la *propriété simple* du modèle *Bell-LaPadula* :

- ***Principe 14* :** la potentialité intrinsèque de la menace *augmente* quand le niveau de confidentialité des objets *augmente*.
- ***Principe 15* :** la potentialité intrinsèque de la menace *augmente* quand le niveau de confidentialité des sujets *diminue*.

La *potentialité intrinsèque de la menace*, des accès en *écriture*, est affectée par les principes suivants qui remplacent la *propriété étoile* du modèle de *Bell-LaPadula* :

- ***Principe 16* :** la potentialité intrinsèque de la menace *augmente* quand le niveau de confidentialité des objets *diminue*.
- ***Principe 17* :** la potentialité intrinsèque de la menace *augmente* quand le niveau de confidentialité des sujets *augmente*.

Rappelons les entités suivantes présentées dans le chapitre *6* :

- un ensemble de *sujets S*.
- un ensemble d'*objets O*.
- un ensemble d'*actions (opérations) A* :
  - *l (lecture)* $\in A$.
  - *e (écriture)* $\in A$.
- un ensemble d'*objectifs de sécurité OB* :
  - *c (confidentialité)* $\in OB$.
  - *i (intégrité)* $\in OB$.
- un ensemble d'instants *T*.

Nous définissons la fonction *Menace_int* : $S \times A \times O \times OB \times T \rightarrow [0, 1]$ qui représente la *potentialité intrinsèque de la menace* de l'exécution d'une action $a \in A$ par un sujet $s \in S$ sur un objet $o \in O$ dans un système qui vise un objectif de sécurité $ob \in OB$, à un instant *t*.

7.2.2.1 Exemples et méthodes d'évaluation de la potentialité intrinsèque de la menace sur la confidentialité

Dans cette section, nous présentons un scénario qui sera utilisé dans le reste du chapitre pour motiver notre approche.

Le *Tableau 32* montre les niveaux de confidentialité à un instant *t* des sujets suivants : s_1 *(chef de projet)*, s_2 *(Ingénieur principal)*, s_3 (*Ingénieu*r), s_4 (*Technicien supérieur*) et s_5 (*Technicien*).

Sujet	***Niveaux de confidentialité à l'instant t***
s_1 *(Chef de projet)*	*10*
s_2 *(Ingénieur principal)*	*9*
s_3 *(Ingénieur)*	*8*
s_4 *(Technicien supérieur)*	*7*
s_5 *(Technicien)*	*6*

Tableau 32. Niveaux de confidentialité des sujets

Le *Tableau 33* montre les niveaux de confidentialité à un instant *t* des objets suivants : o_1 *(Fichiers personnels)*, o_2 *(Fichiers de la planification et du budget)*, o_3 *(Fichiers des courriels)*, o_4 *(Fichiers d'évaluation)* et o_5 *(Fichiers de journalisation)*.

Objet	***Niveaux de confidentialité à l'instant t***
o_1 *(Fichiers personnels)*	*10*
o_2 *(Fichiers planification et budget)*	*9*
o_3 *(Fichiers courriels)*	*8*
o_4 *(Fichiers d'évaluation)*	*7*
o_5 *(Fichiers de journalisation)*	*6*

Tableau 33. Niveaux de confidentialité des objets

Dans cette section, nous adaptons l'approche de l'évaluation de la *potentialité intrinsèque de la menace*, basée sur les objets, que nous avons présentée dans [60, 61]. Cette approche est basée sur les niveaux de confidentialité des objets en premier lieu et les niveaux de confidentialité des sujets en second lieu. Les autres approches présentées dans [60, 61] peuvent être adaptées à l'approche que nous présentons dans cette thèse puisque le cadre conceptuel que nous présentons reste valable.

A. Lecture et confidentialité

Nous présentons dans ce qui suit des exemples qui motivent notre approche pour l'évaluation de la *potentialité intrinsèque de la menace*, dans le cas des accès en *lecture*, où l'objectif de sécurité visé est la *confidentialité*.

Exemple 1 : la *Figure 36* représente les deux demandes d'accès suivantes :

- le sujet s_3, qui a un niveau de confidentialité de *8*, demande l'accès en lecture à l'objet o_1 dont le niveau de confidentialité est *10*.
- le sujet s_4, qui a un niveau de confidentialité de *7*, demande l'accès en lecture à l'objet o_2 dont le niveau de confidentialité est *9*.

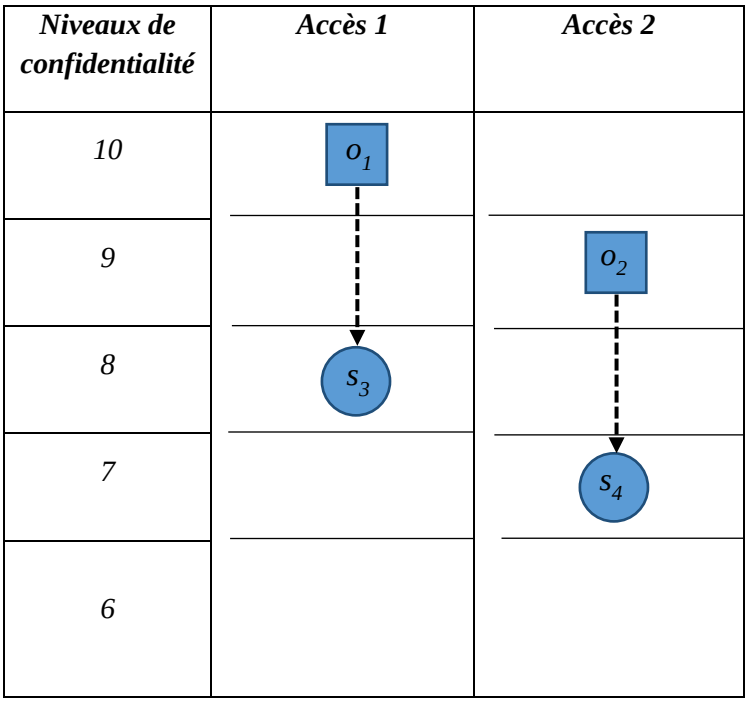


Figure 36. Demandes d'accès décrites dans l'Exemple 1

Le niveau de confidentialité de l'objet est le critère de base pour la détermination de la *potentialité intrinsèque de la menace*. Ainsi, selon le ***Principe 14*** énoncé dans la section 7.*2.3*, autoriser s_3 à accéder en *lecture* à l'objet o_1 donne lieu à une *potentialité intrinsèque de la menace* plus grande qu'autoriser s_4 à accéder en *lecture* à l'objet o_2. Cela est dû au fait que le niveau de confidentialité de l'objet o_1 est plus élevé que celui de l'objet o_2.

Dans l'exemple ci-dessus, nous avons pu déterminer l'accès qui donne lieu à une *potentialité intrinsèque de la menace* plus grande en comparant les niveaux de

confidentialité de deux objets. Cependant, cette technique n'est plus suffisante quand les niveaux de confidentialité des objets sont identiques.

Exemple 2 : étendons l'**Exemple 1** en considérant la demande d'accès suivante représentée dans la *Figure 37* :

- le sujet s_5, qui a un niveau de confidentialité de *6*, demande l'accès en lecture à l'objet o_2 dont le niveau de confidentialité est de *9*.

En d'autres termes, s_4 et s_5 demandent l'accès en lecture à l'objet o_2 dont le niveau de confidentialité est de *9*.

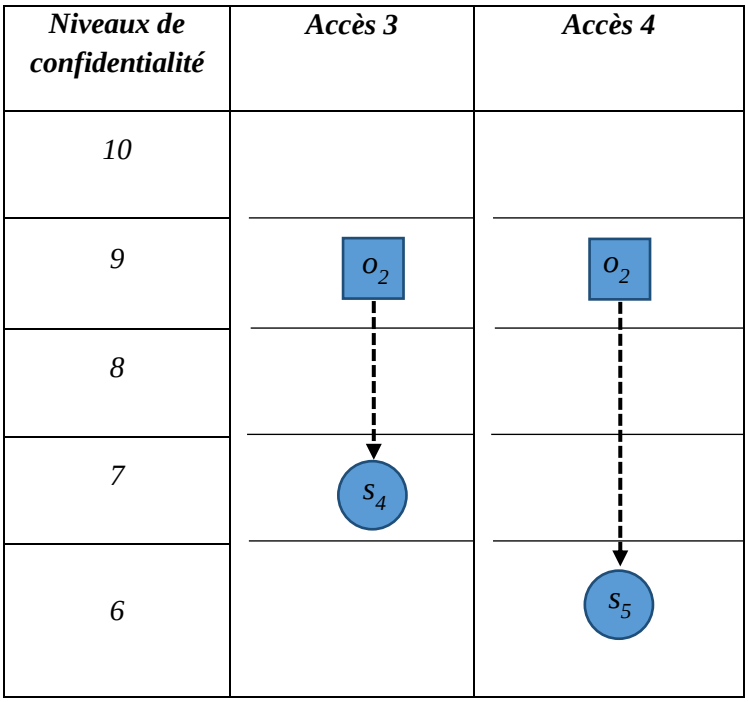


Figure 37. Demandes d'accès décrites dans l'Exemple 2

Selon le ***Principe 15*** énoncé dans la section *7.2.3*, autoriser s_5 à accéder en *lecture* à l'objet o_2 donne lieu à une potentialité intrinsèque de menace *plus grande* qu'autoriser s_4 à accéder en *lecture* à l'objet o_2. Cela est dû au fait que le niveau de confidentialité de s_5 est moins élevé que celui de s_4.

Méthode 8 (d'après les exemples *1* et *2*)

Une approche d'évaluation de la *potentialité de la menace* d'un accès en *lecture* quand les

niveaux de confidentialité des sujets sont inférieurs aux niveaux de confidentialité des objets, doit se conformer à ce qui suit :

1. Appliquer le ***Principe 14*** (La *potentialité intrinsèque de la menace* augmente quand le niveau de confidentialité des objets augmente).
2. Si les niveaux de confidentialité des objets sont égaux alors appliquer le ***Principe 15*** **(**La *potentialité intrinsèque de la menace* augmente quand le niveau de confidentialité des sujets diminue)

Selon la *Méthode 8*, nous obtenons un "ordre de priorité", sur la *potentialité intrinsèque de la menace* pour les demandes d'accès des exemples *1* et *2*, comme suit :

$$Menace\_int(s_4, l, o_2, c, t) < Menace\_int(s_5, l, o_2, c, t) < Menace\_int(s_3, l, o_1, c, t)$$

La *Méthode 8* peut être formalisée comme suit lorsque $csl(s,t) < col(o,t)$ et $csl(s',t) < col(o', t)$:

Menace_int(s, l, o, c, t) < Menace_int(s', l, o',c, t) si :
1. col(o, t) < col(o', t) ou
2. col(o,t) = col(o', t) et csl(s', t) < csl(s, t)

Tableau 34. Évaluation de la *potentialité intrinsèque de la menace* sur la confidentialité dans le cas des accès en lecture

Cette définition permet d'établir un *ordre total* sur les *potentialités intrinsèques de la menace* des requêtes d'accès en lecture quand les sujets et les objets appartiennent à des niveaux différents.

B. Écriture et confidentialité

Nous présentons dans le reste de cette section des exemples qui motivent notre approche pour le calcul de la *potentialité intrinsèque de la menace* dans le cas des accès en *écriture* quand les niveaux de confidentialité des sujets sont supérieurs aux niveaux de confidentialité des objets.

Exemple 3 : soient les deux demandes d'accès suivantes :

- le sujet s_3, qui a un niveau de confidentialité de *8*, demande l'accès en écriture à l'objet o_5 dont le niveau de confidentialité est de *6*.

- le sujet s_2, qui a un niveau de confidentialité de *9*, demande l'accès en écriture à l'objet o_4 dont le niveau de confidentialité est de *7*.

Le niveau de confidentialité de l'objet est le critère de base pour la détermination de la *potentialité intrinsèque de la menace*. Ainsi, selon le ***Principe 16*** énoncé dans la section *7.2.3*, autoriser s_3 à accéder en *écriture* à l'objet o_5 donne lieu à une *potentialité intrinsèque de la menace plus grande* qu'autoriser s_2 à accéder en *écriture* à l'objet o_4. Cela est dû au fait que le niveau de confidentialité de l'objet o_5 est moins élevé que celui de l'objet o_4.

Dans l'exemple ci-dessus, nous pouvons déterminer l'accès ayant la plus grande *potentialité intrinsèque de la menace* en comparant les niveaux de confidentialité de deux objets. Cependant, cette technique n'est plus suffisante quand les niveaux de confidentialité des objets sont identiques.

Exemple 4 : étendons l'**Exemple 3** en considérant l'accès suivant :

- le sujet s_1, qui a un niveau de confidentialité de *10*, demande l'accès en écriture à l'objet o_4 dont le niveau de confidentialité est de *7*.

En d'autres termes, s_1 et s_2 demandent l'accès en écriture à l'objet o_4 dont le niveau de confidentialité est *7*.

Ainsi, selon le ***Principe 17*** énoncé dans la section *7.2.3*, autoriser s_1 à accéder en *écriture* à l'objet o_4 donne lieu à une *potentialité de menace plus grande* qu'autoriser s_2 à accéder en *écriture* à l'objet o_4. Cela est dû au fait que le niveau de confidentialité de s_1 est plus élevé que celui de s_2.

Méthode 9 (d'après les exemples *3* et *4*)

Une technique d'évaluation de la *potentialité intrinsèque de la menace* d'un accès en *écriture* quand les niveaux de confidentialité des sujets sont supérieurs aux niveaux de confidentialité des objets**,** qui est principalement basée sur les niveaux de confidentialité des objets, doit se conformer à ce qui suit :

1. Appliquer le ***Principe 16*** (La *potentialité intrinsèque de la menace* augmente quand le niveau de confidentialité des objets diminue).

2. Si les niveaux de confidentialité des objets sont égaux alors appliquer le ***Principe 17*** **(**La *potentialité intrinsèque de la menace* augmente quand le niveau de confidentialité des sujets augmente)**.**

Selon la *Méthode 9*, l'"ordre de priorité", pour les accès des exemples *3* et *4*, est comme suit :

$Menace\_int(s_2, e, o_4, c, t) < Menace\_int(s_1, e, o_4, c, t) < Menace\_int(s_3, e, o_5, c, t)$.

La *Méthode 9* peut-être formalisée comme suit lorsque $csl(s, t) > col(o, t)$ et $csl(s', t) > col(o', t)$:

$Menace\_int(s, e, o, c, t) < Menace\_int(s', e, o', c, t)$ *si :*
1. $col(o, t) > col(o', t)$ *ou*
2. $col(o, t) = col(o', t)$ *et* $csl(s', t) > csl(s, t)$

Tableau 35. Évaluation de la *potentialité intrinsèque de la menace* sur la confidentialité dans le cas des accès en écriture

7.3 Approche pour l'évaluation de la potentialité intrinsèque de la menace sur l'intégrité

La *potentialité intrinsèque de la menace* dans un système de contrôle d'accès, où l'intégrité est visée, est synonyme de la potentialité intrinsèque de la dégradation de l'intégrité de l'information contenue dans les objets suite à un accès. Rappelons que notre hypothèse essentielle est basée sur l'idée que la *potentialité intrinsèque de la menace* sur l'intégrité augmente lorsque les informations passent à des niveaux d'intégrité supérieurs. En effet, le passage des informations à partir d'objets ayant un niveau d'intégrité bas vers des objets ayant un niveau d'intégrité élevé, dégrade le niveau d'intégrité des informations contenues dans les objets appartenant aux niveaux élevés.

La discussion du cas de l'intégrité est très semblable à celle du cas de la confidentialité, en conséquence nous nous limitons à énoncer les principes essentiels.

La valeur de la *potentialité intrinsèque de la menace*, à un instant *t*, dans le cas d'un système de contrôle d'accès, qui vise l'intégrité, dépend des trois critères suivants :

- l'*action demandée* (*lecture* ou *écriture*),

- le *niveau d'intégrité du sujet* à l'instant *t (isl(s, t)),*
- le *niveau d'intégrité de l'objet* à l'instant *t* (*iol(o, t)).*

7.3.1 Approche pour l'évaluation de la potentialité intrinsèque de la menace sur l'intégrité

Dans cette section, nous expliquons les fondements conceptuels de notre approche de calcul de la *potentialité intrinsèque de la menace* lorsque l'objectif d'intégrité est visé.

7.3.1.1 Hypothèses

Notre approche fait la distinction entre des demandes d'accès qui sont acceptées par défaut et les demandes d'accès où les décisions d'accès dépendent de la valeur calculée du risque.

Accès acceptés par défaut

Si $iol(o, t) \geq isl(s, t)$ alors toutes les demandes d'accès en *lecture* à un instant *t*, par un sujet *s* à un objet *o*, seront autorisées.

Si $iol(o, t) \leq isl(s, t)$ alors toutes les demandes d'accès en *écriture* à un instant *t*, par un sujet *s* à un objet *o*, seront autorisées.

Accès basés sur le risque

Si $iol(o, t) < isl(s, t)$ alors une requête d'accès en *lecture* à un instant *t*, par un sujet *s* à un objet *o*, ne sera autorisée que si le risque qui lui est associé est inférieur au seuil du risque acceptable spécifié.

Si $iol(o, t) > isl(s, t)$ alors une requête d'accès en *écriture* à un instant *t*, par un sujet *s* à un objet *o*, ne sera autorisée que si le risque qui lui est associé est inférieur au seuil de risque acceptable spécifié.

Soient les principes suivants :

***Principe 18* :** la *potentialité intrinsèque de la menace sur l'intégrité* est *non nulle* si et seulement si à un instant *t*, un sujet *s* demande d'accéder en *lecture* à un objet *o*, tel que $isl(s, t) > iol(o, t)$. En d'autre termes, si $isl(s, t) \leq iol(o, t)$, pour toute demande faite à un

instant *t*, par un sujet *s* pour accéder en *lecture* à un objet *o*, la *potentialité intrinsèque de la menace* est *nulle*.

***Principe 19* :** la *potentialité intrinsèque de la menace* sur l'intégrité est *non nulle* si et seulement si à un instant *t*, un sujet *s* demande d'accéder en *écriture* à un objet *o*, tel que $isl(s, t) < iol(o, t)$. En d'autre termes, si $isl(s, t) \geq iol(o, t)$, pour toute demande faite à un instant *t*, par un sujet *s* pour accéder en *écriture* à un objet *o*, la *potentialité intrinsèque de la menace* est *nulle*.

7.3.1.2 Principes pour l'évaluation de la potentialité de la menace sur l'intégrité

La *potentialité intrinsèque* de dégradation de l'intégrité des informations devrait être élevée dans le cas d'un sujet qui a un niveau d'intégrité élevé, à qui on donne accès en *lecture* à des informations ayant un niveau d'intégrité bas. De même, cette *potentialité intrinsèque* devrait être élevée dans le cas d'un sujet qui a un niveau d'intégrité bas à qui on donne accès en *écriture* à un objet ayant un niveau d'intégrité élevé.

La mesure de la *potentialité intrinsèque de la menace* des accès, en *lecture*, est affectée par les principes suivants :

- ***Principe 20* :** la potentialité intrinsèque de la menace *augmente* quand le niveau d'intégrité des objets *diminue*.
- ***Principe 21* :** la potentialité intrinsèque de la menace *augmente* quand le niveau d'intégrité des sujets *augmente*.

La mesure de la *potentialité intrinsèque de la menace*, des accès en *écriture*, est affectée par les principes suivants :

- ***Principe 22* :** la potentialité intrinsèque de la menace *augmente* quand le niveau d'intégrité des objets *augmente*.
- ***Principe 23* :** la potentialité intrinsèque de la menace *augmente* quand le niveau d'intégrité des sujets *diminue*.

Méthode 10

Une approche d'évaluation de la *potentialité intrinsèque de la menace* d'un accès à un

instant *t* en *lecture* quand les niveaux d'intégrité des sujets sont supérieurs aux niveaux d'intégrité des objets, doit se conformer à ce qui suit :

1. Appliquer le ***Principe 20***.
2. Si les niveaux d'intégrité des objets sont égaux alors appliquer le ***Principe 21***.

La *Méthode 10* peut être formalisée comme suit lorsque *isl(s,t) > iol(o,t) et isl(s',t) > col(o,t')* :

Menace_int(s, l, o, i, t) < Menace_int(s', l, o', i, t) si :
1. iol(o, t) > iol(o', t) ou
2. iol(o, t) = iol(o', t) et isl(s', t) > isl(s, t)

Tableau 36. Évaluation de la *potentialité intrinsèque de la menace* sur l'intégrité dans le cas des accès en lecture

Méthode 11

Une approche d'évaluation de la *potentialité intrinsèque de la menace* d'un accès à un instant *t* en *écriture* quand les niveaux d'intégrité des sujets sont inférieurs aux niveaux d'intégrité des objets, doit se conformer à ce qui suit :

1. Appliquer le ***Principe 22***.
2. Si les niveaux d'intégrité des objets sont égaux alors appliquer le ***Principe 23***.

La *Méthode 11* peut être formalisée comme suit lorsque *isl(s,t) < iol(o, t)* et *isl(s',t) < iol(o',t) :*

Menace_int(s, e, o, i, t) <Menace_int(s', e, o', i, t) si:
1. iol(o, t) < iol (o', t) ou
2. iol(o, t) = iol(o', t) et isl(s', t) < isl(s, t)

Tableau 37. Évaluation de la *potentialité intrinsèque de la menace* sur l'intégrité dans le cas des accès en écriture

7.4 Formules pour le calcul de la potentialité de la menace

Dans la section précédente, nous avons décrit une approche pour l'évaluation de la *potentialité intrinsèque de la menace*. Nous avons également discuté la définition d'un *ordre de priorité* sur ces potentialités. Cet ordre de priorité permet une comparaison de la

potentialité de la menace d'un ensemble de demandes d'accès. Par exemple, compte tenu de deux demandes d'accès *(s, a, o, ob, t)* et *(s', a, o', ob, t),* un ordre de priorité de la *potentialité intrinsèque de la menace* peut être utile pour déterminer lequel des accès, a une *potentialité intrinsèque de la menace* plus grande que l'autre. Cela dit, mesurer quantitativement la potentialité *intrinsèque de* la menace serait plus utile. Cependant, il peut y avoir plusieurs formules qui respectent les principes de notre approche et peuvent mesurer quantitativement la *potentialité intrinsèque de la menace* de l'octroi d'un accès. Dans cette section, nous proposons un ensemble de formules et nous décrivons leur construction.

7.4.1 Formule pour le calcul de la potentialité intrinsèque de la menace sur la confidentialité

À partir de cette section, nous introduisons le concept de l'indexation attribuée aux niveaux de confidentialité des sujets et des objets. Nous attribuons une valeur numérique de l'ensemble *{0, ..., |L_c|}* qui représente l'indice de la *potentialité intrinsèque de la menace* d'un sujet ou d'un objet ayant le niveau de confidentialité l_c.

7.4.1.1 Formule pour le calcul de la potentialité intrinsèque de la menace sur la confidentialité des accès en lecture

Dans le cas des accès en lecture lorsque l'objectif de confidentialité est visé, la *potentialité intrinsèque de la menace* augmente lorsque les niveaux de confidentialité des sujets demandeurs d'accès diminuent. Par conséquent, les valeurs des indices de la *potentialité intrinsèque de la menace* des sujets augmentent lorsque leurs niveaux de confidentialité diminuent. Nous écrivons $\widehat{csl(s,\ t)}$ pour désigner l'indice de la *potentialité intrinsèque de la menace* d'un sujet ayant le niveau de confidentialité *csl(s, t)*. Formellement, $\widehat{csl(s,\ t)}$ = *(|L_c| +1) – csl(s, t)*. La deuxième colonne du *Tableau 38* montre l'affectation des indices de la *potentialité intrinsèque de la menace* aux sujets en fonction de leurs niveaux de confidentialité. Par exemple, pour *|L_c| = 5 et csl(s, t) = 4*, $\widehat{csl(s,\ t)} = 2$.

Niveaux de confidentialité des sujets à un instant t	***Indices de la potentialité intrinsèque de la menace des sujets à un instant t***
Non classifié = 1	*5*
Restreint = 2	*4*
Classifié = 3	*3*
Secret = 4	*2*
Top Secret = 5	*1*

Tableau 38. Indices de la *potentialité intrinsèque de la menace* des sujets pour les accès en lecture lorsque la confidentialité est visée

La potentialité intrinsèque de la menace augmente lorsque les niveaux de confidentialité des objets augmentent. Par conséquent, l'indice de la *potentialité intrinsèque de la menace* des objets augmente avec les niveaux de confidentialité des objets. Nous écrivons $\widehat{col(o,\ t)}$ pour désigner l'indice de la *potentialité intrinsèque de la menace* d'un objet ayant le niveau de confidentialité *col(o, t)*. Formellement, $\widehat{col(o,\ t)}$ = *col(o, t)*. La deuxième colonne du *Tableau 39* montre l'affectation des indices de la *potentialité intrinsèque de la menace* des objets en fonction des niveaux de confidentialité des objets. Par exemple, pour $|L_c| = 5$ et *col(o, t) = 4*, $\widehat{col(o,\ t)} = 4$.

Niveau de confidentialité des objets	***Indice de la potentialité intrinsèque de la menace des objets***
Non classifié = 1	*1*
Restreint = 2	*2*
Classifié = 3	*3*
Secret = 4	*4*
Top Secret = 5	*5*

Tableau 39. Indices de la potentialité intrinsèque de la menace des objets pour les accès en lecture lorsque la confidentialité est visée

Dans le cas des accès en lecture lorsque l'objectif de confidentialité est visé, nous proposons la *Formule 7* qui respecte les propriétés de la *Méthode 8* pour mesurer la

potentialité intrinsèque de la menace d'une demande d'accès en lecture d'un sujet *s* à un objet *o* à un instant *t* :

$$Menace\_int(s,l,o,c,t) = \begin{cases} \frac{\left(|L_c| \times \widehat{col(o,\ t)}\right) + \widehat{csl(s,\ t)}}{(|L_c|+1)^2 - 1} & si\ csl(s,t) < col(o,t), \\ 0 \qquad autrement \end{cases}$$

Tableau 40. Formule 7 : calcul de la potentialité intrinsèque de la menace sur la confidentialité dans le cas des accès en lecture

Le numérateur de la *Formule 7* est intuitif. Nous avons besoin d'accorder une plus grande importance à l'indice de la *potentialité intrinsèque de la menace* de l'objet, nous multiplions l'indice de la *potentialité intrinsèque de la menace* de l'objet par $|L_c|$. Ensuite, nous ajoutons l'indice de la *potentialité intrinsèque de la menace* du sujet. Afin d'avoir des valeurs de la *potentialité intrinsèque de la menace* dans l'intervalle [*0, 1*], nous divisons la valeur obtenue à partir du numérateur par $(|Lc| + 1)^2 - 1$. La valeur finale résultante représente la potentialité intrinsèque de la menace basée sur les objets, qui respecte les principes de la *Méthode 8*.

Le *Tableau 41* montre une représentation de la *potentialité intrinsèque de la menace* d'un ensemble d'accès possible en lecture des sujets à des objets. Notons que pour une demande d'accès en lecture d'un sujet *s* à un objet *o*, où $csl(s, t) \geq col(o, t)$ la *potentialité intrinsèque de la menace* est nulle. Ainsi, dans le *Tableau 41*, nous attribuons la valeur *zéro* à tous les accès en lecture au-dessous de la diagonale. Chaque entrée *[k, l]* du tableau comprend une valeur qui représente la *potentialité intrinsèque de la menace* de la demande d'accès en lecture d'un sujet *s* à un objet *o*, où $csl(s, t) = k$ et $col(o, t) = l$. Ces valeurs ont été calculées en utilisant la *Formule 7*. Chaque entrée du tableau contient aussi le « rang de la *potentialité intrinsèque de la menace* » (entre parenthèses) par rapport aux autres accès en lecture, où un rang plus élevé signifie une plus grande *potentialité intrinsèque de la menace*.

Nous pouvons remarquer de chaque ligne dans le *Tableau 41* que les valeurs de la *potentialité intrinsèque de la menace* augmentent à mesure que les niveaux de confidentialité des objets augmentent. Dans chaque colonne, les valeurs de la *potentialité intrinsèque de la menace* augmentent à mesure que les niveaux de confidentialité des sujets

diminuent. Plus précisément, les valeurs de la *potentialité intrinsèque de la menace* les plus bas sont observées pour les objets ayant les niveaux de confidentialité les plus bas, alors que les valeurs de la *potentialité intrinsèque de la menace* les plus élevées sont observées pour les objets ayant les niveaux de confidentialité les plus élevés. En effet, la *potentialité intrinsèque de la menace* la plus élevée est observée pour les sujets ayant des niveaux de confidentialité *1* qui demandent de lire des objets ayant des niveaux de confidentialité *5*.

Niveaux de confidentialité des sujets à un insant t	***Niveaux de confidentialité des objets à un instant t***				
	1	*2*	*3*	*4*	*5*
1	*0*	*0,42(10)*	*0,57(8)*	*0,71(5)*	*0,85(1)*
2	*0*	*0*	*0,54(9)*	*0,68(6)*	*0,82(2)*
3	*0*	*0*	*0*	*0,65(7)*	*0,8(3)*
4	*0*	*0*	*0*	*0*	*0,77(4)*
5	*0*	*0*	*0*	*0*	*0*

Tableau 41. Potentialité intrinsèque de la menace pour les accès en lecture lorsque la confidentialité est visée

Preuve de correction de la *Formule 7*

Cette section montre que la formule de calcul de la *potentialité intrinsèque de la menace Formule 7* satisfait les principes présentés dans ce chapitre. Le graphique représenté dans la *Figure 38* est obtenu par la *Formule 7*. Pour justifier nos choix de construction de cette formule et des autres formules de ce chapitre, nous extrayons le principe suivant de la fonction *Menace_int* : $S \times A \times O \times OB \times T \rightarrow [0, 1]$:

***Principe 24* :** les valeurs de la *potentialité intrinsèquede la menace* sont dans un intervalle [*0,1*].

Le graphique de la *Figure 38* montre que les ***Principes 12***, ***14***, ***15*** et ***24*** sont satisfaits. En effet, pour tout sujet *s* qui demande d'accéder en lecture à un objet *o* à un instant *t* où

csl(s, t) ≥ *col(o, t)*, la figure montre que la *potentialité intrinsèque de la menace* est égale à zéro. Cela satisfait le ***Principe 12*****.** En effet, la *potentialité intrinsèque de la menace* d'une demande d'un sujet *s* pour lire un objet *o*, tel que *csl(s, t)* ≥ *col(o, t)* est nulle, elle est non nulle autrement.

Le côté gauche de la figure montre qu'avec l'augmentation des niveaux de confidentialité des objets et la diminution des niveaux de confidentialité des sujets, la *potentialité intrinsèquede la menace* augmente. Cela satisfait les ***Principes 14*** et ***15***.

Le côté droit de la figure montre qu'avec la diminution des niveaux de confidentialité des objets, et l'augmentation des niveaux de confidentialité des sujets, la *potentialité intrinsèque de la menace* diminue. Cela satisfait les ***Principes 14*** et ***15***.

La figure montre également que les valeurs de la *potentialité intrinsèque de la menace* sont entre *0* et *1*. Cela satisfait le ***Principe 24***.

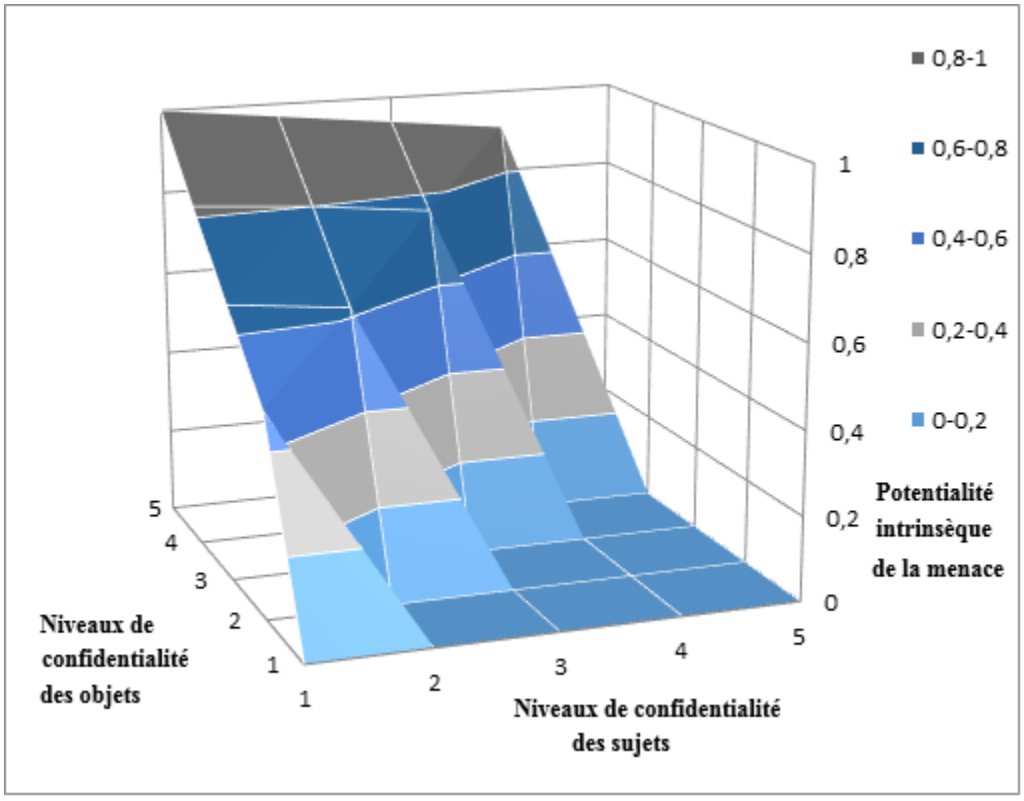


Figure 38. Comportement de valeurs de la *potentialité intrinsèque de la menace* en fonction des niveaux de confidentialité des sujets et des objets

7.4.1.2 Formule pour le calcul de la potentialité intrinsèque de la menace sur la confidentialité des accès en écriture

Dans le cas des accès en écriture lorsque la confidentialité est visée, la *potentialité intrinsèque de la menace* augmente lorsque les niveaux de confidentialité des sujets augmentent. Par conséquent, les valeurs des indices de la *potentialité intrinsèque de la menace* des sujets augmentent avec leurs niveaux de confidentialité. L'indice de *potentialité intrinsèque de la menace* d'un sujet ayant le niveau de confidentialité *csl(s, t)* est $\widehat{csl(s,\ t)}$. La deuxième colonne du *Tableau 42* montre l'affectation des indices de la potentialité intrinsèque de la menace aux sujets. Par exemple, pour *csl(s, t) = 5*, $\widehat{csl(s,\ t)} = 5$.

Niveaux de confidentialité des sujets à un instant t	***Indices de potentialité de la menace des sujets à un instant t***
Non classifié = 1	*1*
Restreint = 2	*2*
Classifié = 3	*3*
Secret = 4	*4*
Top Secret = 5	*5*

Tableau 42. Indices de la *potentialité intrinsèque de la menace* des sujets lors des accès en écriture lorsque la confidentialité est visée

Dans le cas des accès en écriture lorsque la confidentialité est visée, la *potentialité intrinsèque de la menace* augmente lorsque les niveaux de confidentialité des objets diminuent. Par conséquent, les valeurs des indices de la *potentialité intrinsèque de la menace* des objets diminuent avec l'augmentation de leurs niveaux de confidentialité. La deuxième colonne du *Tableau 43* montre l'affectation des indices de la *potentialité intrinsèque de la menace* aux objets. $\widehat{col(o,\ t)}$ dénote l'indice de la *potentialité intrinsèque de la menace* d'un objet. Formellement, $\widehat{col(o,\ t)} = (|L_c| + 1) - col(o, t)$. Par exemple, pour $|L_c| = 5$ et *col(o, t) = 2*, $\widehat{col(o,\ t)} = 4$.

Niveaux de confidentialité des objets à un instant t	***Indices de la potentialité intrinsèque de la menace des objets à un instant t***
Non classifié = 1	*5*
Restreint = 2	*4*
Classifié = 3	*3*
Secret = 4	*2*
Top Secret = 5	*1*

Tableau 43. Indices de la *potentialité intrinsèque de la menace* des objets lors des accès en écriture lorsque la confidentialité est visée

Nous proposons la *Formule 8* qui respecte les propriétés de la *Méthode 9* pour mesurer quantitativement la *potentialité intrinsèque de la menace* de l'accès en écriture d'un sujet *s* à un objet *o*.

$$Menace(s,e,o,c,t) = \begin{cases} \dfrac{(|L_c|+1) \times (\widehat{col(o,\ t)}) + \widehat{csl(s,\ t)}}{(|L_c|+1)^2} & si\ csl(s,t) > col(o,t), \\ 0 & autrement \end{cases}$$

Tableau 44. Formule 8 : calcul de la potentialité intrinsèque de la menace sur la confidentialité dans le cas des accès en écriture

Nous voulons qu'une plus grande importance soit accordée à l'indice de la *potentialité intrinsèque de la menace* des objets, alors nous multiplions $|L_c|+ 1$ par l'indice de la *potentialité intrinsèque de la menace* de l'objet. Ensuite, nous ajoutons l'indice de la *potentialité intrinsèque de la menace* du sujet. Afin d'avoir des valeurs dans un intervalle [*0, 1*], nous divisons la valeur obtenue à partir du numérateur par $(|L_c|+1)^2 - 1$. La valeur résultante représente la *potentialité intrinsèque de la menace*, basée sur les objets, qui respecte les principes de la *Méthode 9*.

Le *Tableau 45* montre une représentation de la *potentialité intrinsèque de la menace* d'un ensemble d'accès possibles en écriture des sujets à des objets. Notons que pour une demande d'accès en écriture d'un sujet *s* à un objet *o*, lorsque $col(o, t) \geq csl(s, t)$ la *potentialité intrinsèque de la menace* est nulle. Ainsi, dans le *Tableau 45*, nous attribuons zéro à tous les accès en écriture au-dessus de la diagonale. Chaque entrée [*i, j*] du tableau

comprend une valeur qui représente la *potentialité intrinsèque de la menace* de la demande d'accès en écriture d'un sujet *s* à un objet *o*, où *csl(s, t) = i* et *col(o, t) = j*. Ces valeurs ont été calculées en utilisant la *Formule 8*. Chaque entrée du tableau contient aussi le « rang de la *potentialité intrinsèque de la menace* » (entre parenthèses) par rapport aux autres accès en écriture, où un rang plus élevé signifie une plus grande *potentialité intrinsèque de la menace*.

Nous pouvons remarquer à partir de chaque ligne dans le *Tableau 45* que les valeurs de la *potentialité intrinsèque de la menace* augmentent à mesure que les niveaux de confidentialité des objets diminuent. Dans chaque colonne, les valeurs de la *potentialité intrinsèque de la menace* augmentent à mesure que les niveaux de confidentialité des sujets augmentent. Les valeurs de la *potentialité intrinsèque de la menace* les moins élevées sont observées pour les objets ayant les niveaux de confidentialité les plus élevés, alors que les valeurs les plus élevées sont observées pour les objets ayant les niveaux de confidentialité les moins élevées. La *potentialité intrinsèque de la menace* la plus élevée est observée pour les sujets ayant des niveaux de confidentialité *5* qui demandent d'écrire dans des objets ayant des niveaux de confidentialité *1*.

Niveaux de confidentialité des sujets	***Niveaux de confidentialité des objets***				
	1	*2*	*3*	*4*	*5*
1	*0*	*0*	*0*	*0*	*0*
2	*0,88(4)*	*0*	*0*	*0*	*0*
3	*0,91(3)*	*0,75(7)*	*0*	*0*	*0*
4	*0,94(2)*	*0,77(6)*	*0,61(9)*	*0*	*0*
5	*0,97(1)*	*0,8(5)*	*0,63(8)*	*0,47(10)*	*0*

Tableau 45. *Potentialité intrinsèque de la menace* pour les accès en écriture lorsque la confidentialité est visée

Notons que la preuve de correction de la *Formule 8* est similaire à celle de la *Formule 7* puisque les principes respectés par la *Formule 8* sont duaux des principes respectés par la *Formule 7*.

7.4.2 Formules pour le calcul de la potentialité intrinsèque de la menace sur l'intégrité

Dans cette section, nous présentons des formules pour l'évaluation de la *potentialité intrinsèque de la menace* lorsque l'intégrité est visée.

7.4.2.1 Formule pour le calcul de la potentialité intrinsèque de la menace sur l'intégrité dans le cas des accès en lecture

Dans le cas des accès en *lecture* lorsque l'intégrité est visée : la *potentialité intrinsèque de la menace* augmente lorsque les niveaux d'intégrité des sujets augmentent et lorsque les niveaux d'intégrité des objets diminuent. Nous proposons la *Formule 9* qui respecte les propriétés de la *Méthode 10* pour mesurer la *potentialité intrinsèque de la menace* d'une demande d'accès en lecture d'un sujet *s* à un objet *o*, où *isl(s, t) > iol(o, t)*. Notons que la *Formule 9* respecte des principes similaires aux principes de la *Formule 8* sauf que la *Formule 9* considère les accès en lecture et les niveaux d'intégrité.

$$Menace(s,l,o,i,t) = \begin{cases} \dfrac{(|L_i|+1) \times (\iota\widehat{ol(o,\ t)}) + \widehat{isl(s,\ t)}}{(|L_i|+1)^2 - 1} & si\ isl(s,t) > iol(o,t), \\ 0 \qquad\qquad autrement \end{cases}$$

Tableau 46. Formule 9 : calcul de la *potentialité intrinsèque de la menace* sur l'intégrité dans le cas des accès en lecture

$\widehat{isl(s,\ t)}$ dénote l'indice de la *potentialité intrinsèque de la menace sur l'intégrité* d'un sujet *s* à un instant *t*. $\widehat{isl(s,\ t)}$ = *isl(s, t).*

$\iota\widehat{ol(o,\ t)}$ dénote l'indice de la *potentialité intrinsèque de la menace sur l'intégrité* d'un objet à un instant *t*. $\iota\widehat{ol(o,\ t)}$ = $|L_i|$ - l_i.

7.4.2.2 Formule pour le calcul de la potentialité intrinsèque de la menace sur l'intégrité dans le cas des accès en écriture

Dans le cas des accès en *écriture* lorsque l'intégrité est visée, la potentialité intrinsèque de la menace augmente lorsque les niveaux d'intégrité des sujets diminuent et lorsque les niveaux d'intégrité des objets augmentent. Nous proposons la *Formule 10* qui respecte les propriétés de la *Méthode 11* pour mesurer la potentialité intrinsèque de la menace d'une demande d'accès en écriture d'un sujet *s* à un objet *o*, où $iol(o) > isl(s)$. Notons que la *Formule 10* respecte des principes similaires aux principes de la *Formule 7* sauf que la *Formule 10* considère les accès en écriture et les niveaux d'intégrité.

$$Menace(s,e,o,i,t) = \begin{cases} \dfrac{(|L_i|+1) \times \widehat{iol(o,\ t)} + \widehat{\imath sl(s,\ t)}}{(|L_i|+1)^2 - 1} & si\ isl(s,t) < iol(o,t), \\ 0 \qquad\qquad autrement \end{cases}$$

Tableau 47. Formule 10 : calcul de la *potentialité intrinsèque de la menace* sur l'intégrité dans le cas des accès en écriture

Les preuves de correction de la *Formule 9* et la *Formule 10* sont similaires aux preuves de correction de la *Formule 7* et la *Formule 8* puisque les principes captés par la *Formule 9* et la *Formule 10* sont respectivement duaux des principes captés par la *Formule 7* et la *Formule 8.*

7.4.3 Calcul de la potentialité de la menace

Dans cette section, nous utilisons la notion de *mesure de sécurité* pour désigner une action, un dispositif, une procédure ou une technique qui réduit la *potentialité de la menace*. Selon [23], une *mesure de la sécurité* est le déploiement d'un ensemble de services de sécurité pour se protéger contre une menace de sécurité. Un synonyme de *mesure de sécurité* est *contrôle de sécurité* [53, 54, 56, 57, 58]. Les *contrôles de sécurité* (journalisation des accès, signatures des politiques d'accès, etc.) sont les garanties prescrites conçues pour protéger la confidentialité, l'intégrité et la disponibilité de l'information qui est traitée, stockée et transmise.

La norme I*SO/CEI 27001* [56] exige une vérification régulière de la sécurité des systèmes d'information. Pour ce faire, l'administrateur de sécurité mesure l'effet des

mesures de sécurité mises en place pour la réduction des risques. Dans ce travail, nous adoptons des concepts de la méthodologie *Méhari* [23] pour intégrer l'effet des *mesures de sécurité* afin de calculer la *potentialité de la menace* des demandes d'accès. Nous considérons que la valeur *de la réduction de la potentialité de la menace*, dans le cas d'une requête d'accès, est la somme des effets des mesures de sécurité réductrices de la *potentialité de la menace* à considérer pour cette requête. La potentialité *de la menace* peut être décrite comme suit : *Potentialité de la menace = Potentialité de la menace intrinsèque – Valeur de la réduction de la potentialité de la menace.*

Les étapes pour calculer la *potentialité de la menace* d'une demande d'accès sont les suivantes :

1. Calcul de *la potentialité intrinsèque de menace* en considérant les flux d'informations qui pourraient résulter si l'accès avait été autorisé.
2. Évaluation de l'effet des *mesures de sécurité (*les mesures structurelles, dissuasives et préventives) qui permettent de réduire la *potentialité de la menace* que pourrait représenter l'autorisation d'un accès.
3. Calcul de *la potentialité de la menace*. Dans cette étape, nous évaluons la potentialité de la concrétisation de la menace (la potentialité de l'apparition du risque de la demande d'accès si cette demande a été autorisée) en considérant l'évaluation des *mesures de sécurité.*

7.4.3.1 Tableaux de l'effet des mesures de sécurité

Dans le cadre de cette thèse, nous nous sommes inspirés de la base de connaissances de Méhari [22] et [23] pour proposer des tableaux qui montrent l'effet des mesures de sécurité pour la réduction de la potentialité intrinsèque de la menace du risque que pourrait représenter un accès. Pour calculer la potentialité de la menace, Méhari [22, 23] propose d'analyser préalablement les mesures de sécurité qui permettent de réduire la potentialité de la menace à savoir les mesures structurelles, les mesures dissuasives et les mesures préventives.

Le *Tableau 48* représente l'effet de chaque mesure de sécurité à considérer dans le cas des accès en lecture par des sujets à des objets lorsque la confidentialité est visée. Notons

que pour une demande d'accès d'un sujet *s* pour lire un objet *o* tel que *csl(s, t) > col(o, t) la potentialité de la menace* est nulle. Chaque entrée du tableau (*[i, i +1[, [j, j +1[)* représente les mesures de sécurité et leurs contributions dans la réduction de la potentialité de la menace d'un accès en lecture d'un sujet *s* à un objet *o*, où *csl(s, t)∈ [i, i +1[* et *col(o, t)∈ [j, j +1[*.

Le *Tableau 49* représente l'effet de chaque mesure de sécurité à considérer dans le cas des accès en lecture par des sujets à des objets lorsque l'intégrité est visée. Notons que pour une demande d'accès d'un sujet *s* pour lire un objet *o* tel que *csl(s, t) < col(o, t) la potentialité de la menace* est nulle. Chaque entrée du tableau (*]i - 1, i],]j -1, j])* représente les mesures de sécurité et leurs contributions dans la réduction de la potentialité de la menace d'un accès en lecture d'un sujet *s* à un objet *o*, où *csl(s, t) ∈]i -1, i]* et *col(o, t) ∈]j - 1, j]*.

Nous pouvons voir à partir de chaque entrée des tableaux que la somme des effets de mesures est comprise entre *0* et *1*. Notons que nous considérons que les mesures de sécurité sont parfaitement mises en œuvre et nous ne considérons pas leurs implémentations partielles qui pourraient être derrière un niveau inférieur de la réduction de la *potentialité de la menace*. Le choix des intervalles d'appartenance des niveaux de confidentialité et d'intégrité mentionnées dans les définitions ci-dessus trouve son explication dans les ***Principes 7*** et ***11*** présentés dans le chapitre *6*. En effet, il ne sera pas possible d'obtenir des niveaux de confidentialité inférieurs au niveau de confidentialité initial le plus bas, et il ne sera pas possible d'obtenir des niveaux de confidentialité supérieurs à $|L_c| + 1$ où $|L_c|$ représente le nombre des niveaux de confidentialité intiaux. De même, il ne sera pas possible d'obtenir des niveaux d'intégrité inférieurs au niveau d'intégrité initial le plus bas moins *1* ($Min(L_i) - 1$) et il ne sera pas possible d'obtenir des niveaux d'intégrité supérieurs à$|L_i|$ quireprésente le nombre des niveaux d'intégrité initiaux.

Exemples :

L'interprétation du contenu de la cellule *([1, 2[, [1, 2[)* dans le *Tableau 48* est comme suit :

1. La mesure m_1 permet de réduire la *potentialité de la menace* sur la confidentialité de *0,05* lorsqu'un sujet ayant un niveau de confidentialité appartenant à l'intervalle

[1, 2[accède en lecture à un objet ayant un niveau de confidentialité supérieur à son niveau, et appartenant à l'intervalle *[1, 2[*.

2. La mesure m_2 permet de réduire la *potentialité de la menace* sur la confidentialité de *0,1* lorsqu'un sujet ayant un niveau de confidentialité appartenant à l'intervalle *[1, 2[* accède en lecture à un objet ayant un niveau de confidentialité, supérieur à son niveau, et appartenant à l'intervalle *[1, 2[*.

L'interprétation du contenu de la cellule *(]4, 5],]2, 3])* dans le *Tableau 49* est comme suit :

1. La mesure m_1 permet de réduire la *potentialité de la menace* sur l'intégrité de *0,05* lorsqu'un sujet ayant un niveau d'intégrité appartenant à l'intervalle *]4, 5]* accède en lecture à un objet ayant un niveau d'intégrité appartenant à l'intervalle *]2, 3]*.
2. La mesure m_2 permet de réduire la *potentialité de la menace* de *0,1* lorsqu'un sujet ayant un niveau d'intégrité appartenant à l'intervalle *]4, 5]* accède en lecture à un objet ayant un niveau d'intégrité appartenant à l'intervalle *]2, 3]* quand l'intégrité est visée.

Niveaux de confidentialité des sujets	***Niveaux de confidentialité des objets***				
	[1, 2[	*[2, 3[*	*[3, 4[*	*[4, 5[*	*[5, 6[*
[1, 2[	*(m_1, l, 0,05, c, pot)* *(m_2, l, 0,1, c, pot)*	*(m_1, l, 0,04, c, pot)* *(m_2, l, 0,1, c, pot)*	*(m_1, l, 0,03, c, pot)* *(m_2, l, 0,1, c, pot)*	*(m_1, l, 0,02, c, pot)* *(m_2, l, 0,1, c, pot)*	*(m_1, l, 0,01, c, pot)* *(m_2, l, 0,1, c, pot)* *(m_3, l, 0,05, c, pot)*
[2, 3[		*(m_1, l, 0,04, c, pot)*	*(m_1, l, 0,03, c, pot)* *(m_2, l, 0,1, c, pot)*	*(m_1, l, 0,02, c, pot)* *(m_2, l, 0,1, c, pot)*	*(m_1, l, 0,01, c, pot)* *(m_2, l, 0,1, c, pot)* *(m_3, l, 0,05, c, pot)*
[3, 4[			*(m_1, l, 0,03, c, pot)* *(m_2, l, 0,1, c, pot)*	*(m_1, l, 0,02, c, pot)* *(m_2, l, 0,1, c, pot)*	*(m_1, l, 0,01, c, pot)* *(m_2, l, 0,1, c, pot)* *(m_3, l, 0,05, c, pot)*
[4, 5[				*(m_1, l, 0,05, c, pot)* *(m_2, l, 0,1, c, pot)*	*(m_1, l, 0,05, c, pot)* *(m_2, l, 0,1, c, pot)* *(m_3, l, 0,05, c, pot)*
[5, 6[					*(m_3, l, 0,05, c, pot)*

Tableau 48. Effet des mesures de sécurité lorsque la confidentialité est visée

Niveaux d'intégrité des sujets	***Niveau d'intégrité des objets***				
	]4, 5]	*]3, 4]*	*]2, 3]*	*]1, 2]*	*]0, 1]*
]4, 5]	*(m_1, l, 0,05, i, pot)* *(m_2, l, 0,1, i, pot)*	*(m_1, l, 0,05, i, pot)* *(m_2, l, 0,1, i, pot)*	*(m_1, l, 0,05, i, pot)* *(m_2, l, 0,1, i, pot)*	*(m_1, l, 0,04, i, pot)* *(m_2, l, 0,1, i, pot)*	*(m_1, l, 0,03, i, pot)* *(m_2, l, 0,1, i, pot)*
]3, 4]		*(m_1, l, 0,05, i, pot)*	*(m_1, l, 0,04, i, pot)* *(m_2, l, 0,1, i, pot)*	*(m_1, l, 0,04, i, pot)* *(m_2, l, 0,1, i, pot)*	*(m_1, l, 0,03, i, pot)* *(m_2, l, 0,1, i, pot)*

Niveaux d'intégrité des sujets	***Niveau d'intégrité des objets***				
	]4, 5]	*]3, 4]*	*]2, 3]*	*]1, 2]*	*]0, 1]*
]2, 3]			*(m_1, l, 0,04, i, pot)* *(m_2, l, 0,1, i, pot)*	*(m_1, l, 0,04, i, pot)* *(m_2, l, 0,1, i, pot)*	*(m_1, l, 0,04, i, pot)* *(m_2, l, 0,1, i, pot)*
]1, 2]				*(m_1, l, 0,04, i, pot)* *(m_2, l, 0,1, i, pot)*	*(m_1, l, 0,04, i, pot)* *(m_2, l, 0,1, i, pot)*
]0, 1]					*(m_1, l, 0,04, i, pot)* *(m_2, l, 0,1, i, pot)*

Tableau 49. Effet des mesures de sécurité lorsque l'intégrité est visée

7.4.3.2 Définitions et principes pour le calcul de la potentialité de la menace

Soient les définitions suivantes :

- *Eff_pot(s, a, o, c, t)* désigne la somme des effets des mesures réductrices de la *potentialité de la menace* sur la confidentialité (mesures structurelles, mesures dissuasives et mesures préventives) à un instant *t*, lorsqu'une action $a \in A$ est exécutée par un sujet *s* sur un objet *o* (*Eff_pot*: $S \times A \times O \times OB \times T \rightarrow [0, 1]$).
- *Eff_pot(s, a, o, i, t)* désigne la somme des effets des mesures réductrices de la potentialité de la menace sur l'intégrité (mesures structurelles, mesures dissuasives et mesures préventives) à un instant *t* lorsqu'une action *a* est exécutée par un sujet *s* sur un objet *o.*

Dans le reste de cette thèse, *Menace(s, a, o, ob, t)* désigne la *potentialité* de *la menace* de l'exécution d'une action $a \in A$ par un sujet $s \in S$ sur un objet $o \in O$ dans un système qui vise un objectif de sécurité $ob \in OB$ à un instant $t \in T$ (*Menace* : $S \times A \times O \times OB \times T \rightarrow [0, 1]$).

Nous formalisons l'attribution de valeurs de la *potentialité de la menace*, dans un premier temps, comme suit :

- *Menace(s, l, o, c, t) = Menace_int(s, l, o, c, t) – Eff_pot(s, l, o, c, t).*
- *Menace(s, e, o, c, t) = Menace_int(s, e, o, c, t) – Eff_pot(s, e, o, c, t).*
- *Menace(s, l, o, i, t) = Menace_int(s, l, o, i, t) – Eff_pot(s, l, o, i, t).*
- *Menace(s, e, o, i, t) = Menace_int(s, e, o, i, t) – Eff_pot(s, e, o, i, t).*

Nous définissons les principes suivants pour le calcul de la *potentialité de la menace* d'une demande d'accès :

- ***Principe 25* :** la *potentialité de la menace* d'une demande d'accès est *égale à zéro*, si l'*effet des mesures de sécurité* correspondant est égal ou supérieur à la valeur de la *potentialité de la menace intrinsèque.*
- ***Principe 26* :** la *potentialité de la menace* d'une demande d'accès *augmente* quand la *potentialité de la menace intrinsèque* augmente.
- ***Principe 27* :** la *potentialité de la menace* d'une demande d'accès *augmente* quand l'*effet des mesures de sécurité* correspondant diminue.

- ***Principe 28* :** la valeur de la *potentialité de la menace* d'une demande d'accès est entre *0* et *1*.

Dans ce qui suit, nous présentons des définitions raffinées des formules de calcul de la *potentialité de la menace*. Nous proposons la formule suivante qui permet de capter les principes ci-dessus, permettant ainsi de calculer la *potentialité de la menace* sur la confidentialité d'un accès en lecture par un sujet *s* à un objet *o* tout en considérant les mesures de sécurité mises en place.

$$Menace(s,l,o,c,t) =$$

$$\begin{cases} Menace\_int(s,l,o,c,t) \ - \ Eff\_pot(s,l,o,c,t) \ \ si \ csl(s,t) < col(o,t) \ \ et \\ Eff\_pot(s,l,o,c,t) \ < \ Menace\_int(s,l,o,c,t) \\ 0 \qquad\qquad\qquad autrement \end{cases}$$

Tableau 50. Formule 11 : calcul de la *potentialité de la menace sur la confidentialité* d'un accès en lecture

Notons que la valeur obtenue en appliquant la *Formule 11* est égale au résultat obtenu par la *Formule 7* duquel on soustrait l'*effet des mesures de sécurité réductrices de la potentialité de la menace*. Des formules qui tiennent compte de mesures de sécurité peuvent être développées pour les *Formules 8*, *9* et *10* comme suit :

$$Menace(s,e,o,c,t) =$$

$$\begin{cases} Menace\_int(s,e,o,c,t) \ - \ Eff\_pot(s,e,o,c,t) \ \ si \ csl(s,t) > col(o,t) \ \ et \\ Eff\_pot(s,e,o,c,t) \ < \ Menace\_int(s,e,o,c,t) \\ 0 \qquad\qquad\qquad autrement \end{cases}$$

Tableau 51. Formule 12 : calcul de la potentialité de la menace sur la confidentialité d'un accès en écriture

$$Menace(s,e,o,i,t) =$$

$$\begin{cases} Menace\_int(s,e,o,i,t) \ - \ Eff\_pot(s,e,o,i,t) \ \ si \ isl(s,t) < iol(o,t) \ \ et \\ Eff\_pot(s,e,o,i,t) \ < \ Menace\_int(s,e,o,i,t) \\ 0 \qquad\qquad\qquad autrement \end{cases}$$

Tableau 52. Formule 13 : calcul de la potentialité de la menace sur l'intégrité d'un accès en lecture

$$Menace(s,l,o,i,t) =$$

$$\begin{cases} Menace\_int(s,l,o,i,t) \ - \ Eff\_pot(s,l,o,i,t) \ \ si \ isl(s,t) > iol(o,t) \ \ et \\ Eff\_pot(s,l,o,i,t) < \ Menace\_int(s,l,o,i,t) \\ 0 \qquad\qquad\qquad autrement \end{cases}$$

Tableau 53. Formule 14 : calcul de la potentialité de la menace sur l'intégrité d'un accès en écriture

7.4.3.3 Preuve de correction

Le graphique représenté par la *Figure 39* peut être obtenu par les *Formules 11, 12, 13* ou *14*. Ce graphique montre que les ***Principes 25***, ***26***, ***27*** et ***28*** sont satisfaits. La figure montre que la *potentialité de la menace* d'une demande d'accès est égale à *zéro*, si la valeur des *mesures de sécurité* correspondants est supérieure ou égale à la valeur de la *potentialité intrinsèque de la menace*. Cela satisfait le ***Principe 25***.

Le côté gauche de la figure montre qu'avec l'augmentation de la potentialité intrinsèque et la diminution des valeurs des contre-mesures, la potentialité de la menace augmente. Cela satisfait les ***Principes 26*** et ***27***.

Le côté droit de la figure montre qu'avec la diminution de la potentialité intrinsèque de la menace d'une demande d'accès et l'augmentation des valeurs des contre-mesures correspondant, la potentialité de la menace diminue. Cela satisfait les ***Principes 26*** et ***27.***

La figure montre que les valeurs de la potentialité de la menace des demandes d'accès sont entre *0* et *1*. Cela satisfait le ***Principe 28***.

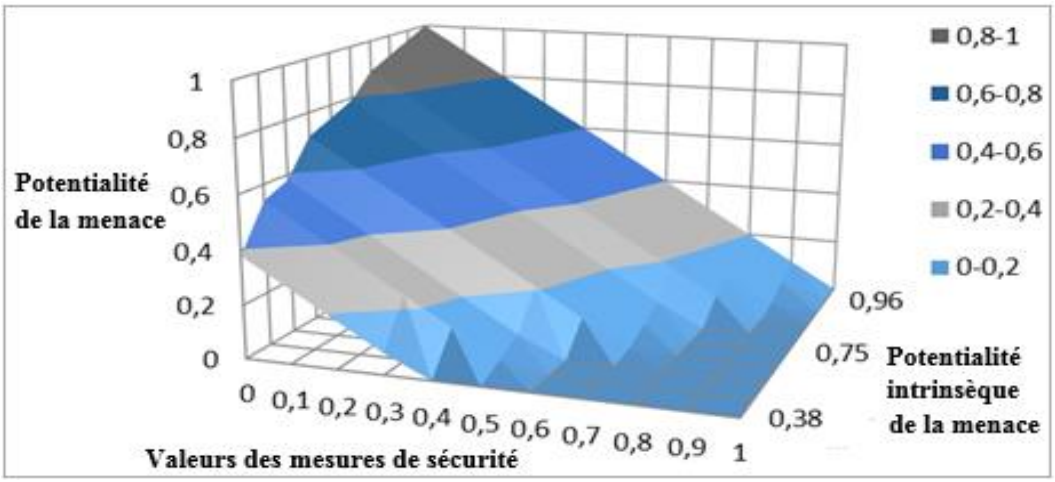


Figure 39. Comportement de valeurs de potentialité de menace en fonction des contremesures et la potentialité intrinsèque de la menace

7.4.3.4 Cas d'utilisation

Supposons qu'un employé *s* ayant un niveau de confidentialité *2,45* demande d'accéder à un objet *o* ayant un niveau de confidentialité *3,22*. Selon le *Tableau 48*, nous considérons l'entrée (*[2, 3[, [3, 4[)* qui indique que les mesures de sécurité m_1 et m_2 peuvent réduire la *potentialité de la menace* de cette demande d'accès de *0,13* (*0,13 = 0,1 + 0,03*). Supposons également que la mesure m_1 consiste à journaliser tous les accès et que la mesure m_2 consiste à faire les employés signer une *politique sur l'accès à l'information*. Étant donné que cet employé n'a pas signé la *politique sur l'accès à l'information*, la réduction de la potentialité de la menace qu'apporte cette *mesure de sécurité* ne sera pas considérée pour le calcul de la valeur finale de la potentialité de la menace sur la confidentialité de l'accès cité dans ce cas d'utilisation. Cette valeur sera donc de *0,1* seulement.

$$Menace(s, l, o, c, t) = \frac{\left(|L_c| \times \widehat{col(o,\ t)}\right) + \widehat{csl(s,\ t)}}{(|L_c|+1)^2-1} - Eff\_pot(s, l, o, c, t)$$

$$= \frac{(6 \times 3{,}22)+((5+1) - 2{,}45)}{35} - 0{,}1$$

$$= 0{,}46$$

7.5 Discussion

Dans cette section, nous comparons notre travail à des travaux remarquables de la littérature et nous présentons les limites de notre approche.

7.5.1 Travaux connexes

Dans nos travaux précédents [60, 61], nous avons présenté une approche pour l'évaluation de la potentialité des menaces des demandes d'accès, qui comprend quatre approches différentes. Dans ce travail, notre approche d'évaluation de la *potentialité de la menace* est basée sur les flux d'informations, fait une distinction entre les accès en lecture et les accès en écriture, donne des estimations basées sur les critères de sécurité (confidentialité ou intégrité), et intègre l'évaluation des mesures de sécurité.

Cheng et al [20] ont proposé une logique floue pour les systèmes de sécurité multi-niveaux (*Fuzzy MLS*), qui quantifie le risque d'une demande d'accès dans les systèmes de sécurité multi-niveaux en multipliant la *valeur de l'information* par la *potentialité de la divulgation non autorisée* des informations. Cette approche considère le concept de la *tentation de divulgation* de l'information et vise à quantifier son risque. Cette approche se limite à l'évaluation de la *potentialité de la menace* des accès en lecture interdits par *Bell-Lapadula* et se limite à l'objectif de la confidentialité. Notre approche permet également d'évaluer la *potentialité de la menace* des accès en lecture et en écriture et pourrait être applicable lorsque l'objectif de l'intégrité est visé.

Bartsch [7] a proposé une approche pour l'évaluation qualitative des risques dans le contexte des systèmes de contrôle d'accès basé sur les rôles *RBAC* [3]. Dans cette approche, le risque est égal à la valeur la plus élevée des valeurs évaluées pour chaque objectif de sécurité (confidentialité, intégrité et disponibilité). Ce travail présente également une méthode pour l'évaluation qualitative de la *potentialité de la menace*. En comparaison avec le travail de *Bartsch*, notre approche est élaborée dans le cadre des systèmes de contrôle d'accès génériques en se référant à la sensibilité des objets et la fiabilité des sujets et ne se limite pas à *RBAC*.

Diep et *al* [29] ont présenté un modèle de contrôle d'accès où les décisions d'accès sont basées sur une évaluation quantitative des risques. Cependant, ce travail ne présente pas une quantification de la *potentialité de la menace*.

Wang et *al* [97] ont proposé une méthode pour quantifier le risque d'accès en tenant compte du *besoin de savoir* et des exigences de protection de la vie privée dans le contexte des systèmes d'information de santé. Ce travail exploite le concept d'entropie de la théorie de l'information pour calculer des valeurs de risque des demandes d'accès. Nous croyons que notre approche pourrait être étendue afin de tenir compte des exigences du besoin de savoir.

Kandala et *al* [59] ont élaboré un cadre qui capte les différents composants et leurs interactions afin de développer "des modèles abstraits" pour *RADAC*. Toutefois, ce travail ne considère pas l'évaluation de la *potentialité de* la *menace* ou du risque.

7.5.2 Limites

L'évaluation de la *potentialité de la menace* des demandes d'accès proposée dans notre approche est basée sur une attribution a priori des niveaux de sécurité aux sujets et aux objets. Cela signifie que le cadre proposé ne peut pas couvrir des menaces qui nécessitent la prise en considération d'autres paramètres tels que les facteurs sociotechniques pour refléter la réalité des menaces internes, à savoir le comportement des utilisateurs, la collusion avec d'autres utilisateurs, etc. Tous ces paramètres sont hors de la portée de ce chapitre. De même, les menaces liées à l'ingénierie sociale, les dénis de service (*DoS*) et les menaces qui pourraient compromettre la disponibilité des données ne peuvent pas être évaluées par notre approche. En outre, les menaces d'infection par les chevaux de Troie qui pourraient résulter du non respect des règles des modèles de contrôle d'accès obligatoire *MAC* [65], ne sont pas considérées.

7.6 Conclusion

Dans ce chapitre, nous avons défini des principes pour déterminer un *ordre de priorité* sur les *potentialités des menaces* des accès. Ces principes se basent sur les niveaux de sécurité des sujets et des objets, et les flux d'informations. En effet, la *potentialité de la menace sur la confidentialité* des informations augmente lorsqu'un accès peut causer un flux d'information vers le bas. Tandis que la *potentialité de la menace sur l'intégrité* augmente dans le cas inverse.

Nous avons présenté également des formules qui captent les principes présentés, et permettent de mesurer quantitativement la potentialité de la menace tout en tenant compte de l'objectif de sécurité (confidentialité, intégrité) visé. De plus, nous avons adopté des concepts de la méthodologie *Méhari* [23] pour intégrer l'évaluation des *mesures de sécurité* qui permettent de réduire la valeur de la *potentialité de la menace.*

À notre connaissance, notre travail représente l'une des rares tentatives dans la littérature de mener une évaluation de la *potentialité de la menace* des demandes d'accès qui est basée sur les flux de l'information et qui considère les mesures de sécurité. Nous avons présenté plusieurs exemples qui justifient notre approche en termes intuitifs. Comme mentionné

dans la section 7.*1*, l'évaluation de la potentialité de la menace est un prérequis pour estimer les risques d'accès. Cependant, notre objectif ultime est de développer un cadre pour estimer le risque de demandes d'accès.

Nous pensons que notre approche peut être facilement modifiée pour tenir compte d'autres critères présentés dans [60, 61]. Ainsi, les principes présentés dans ce chapitre peuvent être considérés comme étant seulement des exemples d'un cadre plus général et peuvent être instanciés de plusieurs manières différentes. Ce cadre peut être utilisé pour évaluer les potentialités de menaces qui seront ensuite utilisés pour calculer les risques. Notons que notre cadre pourrait être étendu pour considérer également les exigences du *besoin de savoir* pour évaluer les potentialités de menaces en tenant compte de la notion de catégories [27].

Dans le chapitre suivant, nous prolongeons les travaux rapportés dans ce chapitre afin de quantifier le risque de demandes d'accès.

Chapitre 8 : Calcul de l'impact

8.1 Introduction

Dans ce chapitre, nous proposons une approche pour le calcul de l'impact des requêtes d'accès. De façon générale, l'impact représente la gravité des conséquences directes et indirectes qui découleraient de l'occurrence du risque suite à un accès autorisé, l'occurrence du risque étant la divulgation ou l'altération des informations [23]. La gravité des conséquences de l'occurrence du risque dépend de l'importance de la confidentialité ou de l'intégrité des informations contenues dans les objets et de l'importance de la confidentialité ou de l'intégrité des informations connues par les sujets. Cet indicateur qui est l'importance de la confidentialité ou de l'intégrité, est reflété par les niveaux de confidentialité et les niveaux d'intégrité des sujets et des objets. Dans cette thèse, nous calculons l'impact de la violation de la politique de contrôle d'accès suite à un accès permis.

Exemple : la conséquence de la violation de la politique de contrôle d'accès, suite à l'autorisation d'accès en lecture à un fichier contenant des informations confidentielles telles des secrets industriels, pourrait être la perte d'un avantage concurrentiel.

Le calcul de l'impact passe par le calcul de l'*impact intrinsèque* qui est une évaluation maximaliste de la possibilité de l'occurrence du risque, sans la considération des mesures de sécurité [23]. L'impact dans notre approche peut être décrit comme suit : *Impact = Impact intrinsèque – Valeur de la réduction de l'impact*.

Ce chapitre est organisé comme suit : la section *2* décrit notre approche pour le calcul de l'impact intrinsèque. La section *3* présente les catégories des mesures de sécurité réductrices de l'impact. Dans la section *4*, nous décrivons notre approche pour le calcul de l'impact et nous présentons des formules à cette fin. Nous concluons dans la section *5* par présenter les contributions ce chapitre et l'intérêt de leur utilisation dans cette thèse.

8.2 Calcul de l'impact intrinsèque

La divulgation des informations confidentielles pourrait être le résultat d'un accès en lecture lorsqu'un sujet lit des informations confidentielles à partir d'un objet ayant un niveau de confidentialité supérieur ou d'un accès en écriture lorsqu'un sujet transmet des informations confidentielles à un objet ayant un niveau de confidentialité inférieur. Pour cela, nous considérons dans notre approche que la valeur de l'*impact intrinsèque* est *proportionnelle* au niveau de confidentialité de l'objet à accéder dans le cas des accès en lecture, étant donné que ce sont les informations contenues dans l'objet qui pourraient être divulguées, et au niveau du sujet demandeur de l'accès dans le cas des accès en écriture puisque ce sont les informations connues par le sujet qui pourraient être divulguées. Autrement dit, c'est le niveau de confidentialité de l'entité *source de l'information* qui est considéré.

La diminution des niveaux d'intégrité des objets pourrait être le résultat d'un accès en lecture lorsqu'un sujet lit des informations ayant un niveau d'intégrité faible ou d'un accès en écriture lorsqu'un sujet transmet des informations ayant un niveau d'intégrité faible à un objet ayant un niveau d'intégrité élevé. Pour cela, nous considérons dans notre approche que la valeur de l'*impact* intrinsèque est *inversement proportionnelle* au niveau d'intégrité de l'objet à accéder dans le cas des accès en lecture puisque ce sont les informations contenues dans l'objet qui pourraient dégrader le niveau d'intégrité du sujet, et au niveau d'intégrité du sujet demandeur de l'accès dans le cas des accès en écriture puisque ce sont les informations connues par le sujet qui pourraient diminuer le niveau d'intégrité de l'objet à accéder. Autrement dit, la gravité des conséquences de la violation de la politique de contrôle d'accès suite à un accès et conséquemment de l'impact intrinsèque, augmente avec la diminution du niveau d'intégrité de l'entité *source de l'information.*

Exemple : l'*impact intrinsèque* de l'autorisation d'accès en écriture à un fichier contenant des informations ayant un niveau d'intégrité élevé telles les informations de suivi de l'état de santé d'un patient, est la dégradation de la fiabilité de son contenu. Cela pourrait engendrer la prescription de médicaments non convenables pour un patient mettant ainsi sa santé en péril.

8.3 Catégories des mesures de sécurité réductrices de l'impact

Le calcul de l'*impact* d'un accès passe par l'évaluation de l'effet des mesures d'*atténuation* de l'*impact*. *La* méthodologie *Méhari* [22, 23] distingue trois catégories de ces mesures de sécurité :

1. Les mesures *protectives* : ces mesures réduisent les conséquences directes d'un risque qui peuvent s'étendre et se propager. Moins ces conséquences sont confinées, plus le risque est grand. **Exemple :** les mesures de détection (p. ex. l'activation de la journalisation des accès) qui permettent une réaction rapide face à un incident de sécurité.
2. Les mesures *palliatives* : ces mesures limitent les conséquences indirectes d'un risque. En effet la situation de crise engendrée par l'occurrence d'un risque peut être anticipée et préparée. Moins cette situation de crise est préparée, plus le risque est grand. **Exemple :** les copies de sauvegarde.
3. Les mesures *récupératives* : ces mesures permettent de réduire l'impact des pertes finales. **Exemple :** l'analyse spécifique des risques à couvrir par l'assurance et la préparation spécifique des actions en justice.

8.4 Calcul de l'impact

L'e*ffet de la réduction de l'impact* dans le cas d'une requête d'accès désigne la somme des effets des mesures de sécurité réductrices de l'*impact* à considérer dans le cas de cette requête. Dans notre approche, l'impact est décrit comme suit : *Impact = Impact intrinsèque – Effet de la réduction de l'impact*. Dans le reste de ce chapitre, *Impact(s, a, o, ob, t) désigne* l'impact de l'exécution d'une action *a* par un sujet *s* sur un objet *o* dans un système qui vise un objectif de sécurité *ob*, à un instant *t*.

Les valeurs de l'impact sont obtenues en soustrayant l'effet des mesures de réduction de l'impact de la valeur de l'impact intrinsèque. Pour calculer l'*impact intrinsèque*, nous considérons que sa valeur est proportionnelle au niveau de confidentialité de l'entité (sujet ou objet) *source de l'information* dans le cas de la confidentialité. Elle est *inversement proportionnelle* au niveau d'intégrité de l'entité (sujet ou objet) *source de l'information*

dans le cas de l'intégrité. Pour que les valeurs de l'impact soient comprises entre *0* et *1*, nous divisons la valeur du niveau de sécurité par *6* dans le cas de la confidentialité. 6 est l'entier le plus petit qui est strictement supérieur au niveau de confidentialité maximum qui peut être obtenu par notre approche lorsque nous considérons *5* niveaux de confidentialité initiaux. Dans le cas de l'intégrité, nous divisons par *5* qui est égale au niveau d'intégrité maximum qui peut être obtenu par notre approche lorsque nous considérons *5* niveaux d'intégrité initiaux.

Dans le cadre de cette thèse, nous nous sommes inspirés de la base de connaissances de *Méhari* [22] et [23] pour proposer des tableaux qui montrent le niveau d'efficacité des mesures de sécurité pour la réduction de l'*impact* que pourrait représenter un accès.

Le *Tableau 54* et le *Tableau 55* présentent respectivement l'efficacité des mesures de sécurité mises en place pour la réduction de l'impact intrinsèque lorsque la confidentialité est visée et lorsque l'intégrité est visée.

Niveau de confidentialité des sujets	***Niveau de confidentialité des objets***				
	[1, 2[	*[2, 3[*	*[3, 4[*	*[4, 5[*	*[5, 6[*
[1, 2[	*(m_1, l, 0,07, c, imp)* *(m_2, l, 0,2, c, imp)* *(m_3, l, 0,08, c, imp)* *(m_4, l, 0,1, c, imp)*	*(m_1, l, 0,06, c, imp)* *(m_2, l, 0,2, c, imp)* *(m_3, l, 0,05, c, imp)* *(m_4, l, 0,1, c, imp)*	*(m_1, l, 0,05, c, imp)* *(m_2, l, 0,1, c, imp)* *(m_3, l, 0,05, c, imp)* *(m_4, l, 0,1, c, imp)*	*(m_1, l, 0,05, c, imp)* *(m_2, l, 0,1, c, imp)* *(m_3, l, 0,05, c, imp)* *(m_4, l, 0,1, c, imp)*	*(m_1, l, 0,05, c, imp)* *(m_2, l, 0,1, c, imp)* *(m_3, l, 0,05, c, imp)* *(m_4, l, 0,1, c, imp)*
[2, 3[		*(m_1, l, 0,07, c, imp)* *(m_2, l, 0,2, c, imp)* *(m_3, l, 0,05, c, imp)* *(m_4, l, 0,1, c, imp)*	*(m_1, l, 0,05, c, imp)* *(m_2, l, 0,1, c, imp)* *(m_3, l, 0,05, c, imp)* *(m_4, l, 0,1, c, imp)*	*(m_1, l, 0,05, c, imp)* *(m_2, l, 0,1, c, imp)* *(m_3, l, 0,05, c, imp)* *(m_4, l, 0,1, c, imp)*	*(m_1, l, 0,05, c, imp)* *(m_2, l, 0,1, c, imp)* *(m_3, l, 0,05, c, imp)* *(m_4, l, 0,1, c, imp)*
[3, 4[			*(m_1, l, 0,05, c, imp)* *(m_2, l, 0,1, c, imp)*	*(m_1, l, 0,05, c, imp)* *(m_2, l, 0,1, c, imp)*	*(m_1, l, 0,05, c, imp)* *(m_2, l, 0,1, c, imp)*

			(m_3, l, 0,05, c, imp) *(m_4, l, 0,1, c, imp)*	*(m_3, l, 0,05, c, imp)* *(m_4, l, 0,1, c, imp)*	*(m_3, l, 0,05, c, imp)* *(m_4, l, 0,1, c, imp)*
[4, 5[				*(m_1, l, 0,05, c, imp)* *(m_2, l, 0,1, c, imp)* *(m_3, l, 0,05, c, imp)* *(m_4, l, 0,1, c, imp)*	*(m_1, l, 0,05, c, imp)* *(m_2, l, 0,1, c, imp)* *(m_3, l, 0,05, c, imp)* *(m_4, l, 0,1, c, imp)*
[5, 6[					*(m_1, l, 0,05, c, imp)* *(m_2, l, 0,1, c, imp)* *(m_3, l, 0,05, c, imp)* *(m_4, l, 0,1, c, imp)*

Tableau 54. Effet des mesures de sécurité réductrices de l'impact dans le cas de la confidentialité

Niveau d'intégrité des sujets	***Niveau d'intégrité des objets***				
	]4,5]	*]3,4]*	*]2,3]*	*]1,2]*	*]0,1]*
]4,5]	*(m_5, l, 0,25, i, imp)*	*(m_5, l, 0,25, i, imp)*	*(m_5, l, 0,25, i, imp)*	*(m_5, l, 0,25, i, imp)*	*(m_5, l, 0,25, i, imp)*
]3,4]		*(m_5, l, 0,25, i, imp)*	*(m_5, l, 0,25, i, imp)*	*(m_5, l, 0,25, i, imp)*	*(m_5, l, 0,25, i, imp)*
]2,3]			*(m_5, l, 0,25, i, imp)*	*(m_5, l, 0,25, i, imp)*	*(m_5, l, 0,25, i, imp)*
]1,2]				*(m_5, l, 0,25, i, imp)*	*(m_5, l, 0,3, i, imp)*
]0,1]					*(m_5, l, 0,3, i, imp)*

Tableau 55. Effet des mesures de sécurité réductrices de l'impact dans le cas de l'intégrité

Par exemple, le contenu de la cellule *(]4, 5],]2, 3])* dans le *Tableau 55*, (*m_5, l, 0,25, i, imp*) signifie que la mesure *m_5* permet de réduire l'*impact* de *0,25* lorsqu'un sujet ayant un

niveau d'intégrité appartenant à l'intervalle *]4, 5]* accède en lecture à un objet ayant un niveau d'intégrité appartenant à l'intervalle *]2, 3]* quand l'intégrité est visée.

Les mesures de sécurité spécifiques et la détermination de leur contribution dans la réduction de la potentialité de la menace et de l'impact pourraient être déterminés par un expert en sécurité de l'information. À noter que les valeurs données dans ce tableau sont données seulement à titre d'exemple. Aussi, nous ne spécifions pas quelles pourraient être les mesures m_1, m_2, m_3, m_4 et m_5.

Soient les fonctions suivantes :

- *Eff_imp(s, a, o, c, t)* désigne la somme de l'efficacité des mesures permettant la réduction de l'impact lorsqu' à un instant *t*, une action *a* est exécutée par un sujet *s*, ayant un niveau de confidentialité appartenant à un intervalle *[j, j + 1[*, sur un objet *o*ayant un niveau de confidentialité appartenant à un intervalle *[k, k + 1[* dans un système qui vise la confidentialité. *j* et *k* représentent des niveaux de confidentialité initiaux. Le choix des bornes de l'intervalle s'explique par le fait que le niveau de confidentialité maximum que nous pouvons obtenir avec notre approche est strictement inférieur au niveau de confidentialité initial maximal plus *1 (5+1)*. En même temps, il ne peut pas être inférieur au niveau de confidentialité initial minimum (*1*).

- *Eff_imp(s, a, o, i, t)* désigne la somme de l'efficacité des mesures permettant la réduction de l'impact lorsqu'à un instant *t*, une action *a* est exécutée par un sujet *s*, ayant un niveau d'intégrité appartenant à un intervalle *]p-1, p]* sur un objet *o* ayant un niveau d'intégrité appartenant à un intervalle *]q-1, q]* dans un système qui vise l'intégrité. *p* et *q* représentent des niveaux d'intégrité initiaux. Le choix des bornes de l'intervalle s'explique par le fait que le niveau d'intégrité maximum que nous pouvons obtenir avec notre approche ne peut pas être inférieur au niveau initial minimum d'intégrité moins *1 (1-1)*. En même temps, le niveau d'intégrité maximal que nous pouvons obtenir est égal au niveau initial maximum d'intégrité (*5*).

- *Impact_int(s, a, o, ob, t)* représente la valeur de l'impact intrinsèque de l'exécution de l'action *a* par un sujet *s* sur un objet *o*, à un instant *t*, lorsque l'objectif de sécurité *ob* est visé.

Les valeurs d'impact intrinsèque sont calculées comme suit :

$Impact\_int(s, l, o, c, t) = col(o, t)/6$

Tableau 55. Formule 15 : calcul de l'impact intrinsèque sur la confidentialité dans le cas des accès en lecture

$Impact\_int(s, e, o, c, t) = csl(s, t)/6$

Tableau 56. Formule 16 : calcul de l'impact intrinsèque sur la confidentialité dans le cas des accès en écriture

$Impact\_int(s, l, o, i, t) = (\|L_i\| - iol(o, t))/5$

Tableau 57. Formule 17 : calcul de l'impact intrinsèque sur l'intégrité dans le cas des accès en lecture

$Impact\_int(s, e, o, i, t) = (\|L_i\| - isl(s, t))/5$

Tableau 58. Formule 18 : calcul de l'impact intrinsèque sur l'intégrité dans le cas des accès en écriture

$|L_i|$ est le nombre de niveaux d'intégrité initiaux qui est égale à *5* dans les exemples de cette thèse.

Pour obtenir des valeurs d'impact intrinsèque comprises entre *0* et *1*, dans le cas de la confidentialité, nous divisons le niveau de confidentialité d'un sujet ou d'un objet par *6* puisque la valeur maximale du niveau de confidentialité s'approche de *6* même si elle ne l'atteint pas. Dans le cas de l'intégrité, la valeur de l'impact est égale au nombre de niveaux d'intégrité initiaux duquel on soustrait le niveau d'intégrité d'un sujet ou d'un objet avant de le diviser par *5* puisque la valeur maximale d'un niveau d'intégrité est égale à *5*.

Les valeurs d'*impact* sont obtenues en soustrayant les effets des mesures de sécurité comme suit :

$$Impact(s,l,o,c,t) =$$

$$\begin{cases} Impact\_int(s,l,o,c,t) \ - \ Eff\_imp(s,l,o,c,t) \ si \ Eff\_imp(s,l,o,c,t) \ < \ Impact\_int(s,l,o,c,t) \\ 0 \qquad\qquad autrement \end{cases}$$

Tableau 59. Formule 19 : calcul de l'impact sur la confidentialité dans le cas des accès en lecture

$$Impact(s,e,o,c,t) =$$

$$\begin{cases} Impact\_int(s,e,o,c,t) \ - \ Eff\_imp(s,e,o,c,t) \ si \ Eff\_imp(s,e,o,c,t) \ < \ Impact\_int(s,e,o,c,t) \\ 0 \qquad\qquad autrement \end{cases}$$

Tableau 60. Formule 20 : calcul de l'impact sur la confidentialité dans le cas des accès en écriture

$$Impact(s,l,o,i,t) =$$

$$\begin{cases} Impact\_int(s,l,o,i,t) \ - \ Eff\_imp(s,l,o,i,t) \ si \ Eff\_imp(s,l,o,i,t) \ < \ Impact\_int(s,l,o,i,t) \\ 0 \qquad\qquad autrement \end{cases}$$

Tableau 61. Formule 21 : calcul de l'impact sur l'intégrité dans le cas des accès en lecture

$$Impact(s,e,o,i,t) =$$

$$\begin{cases} Impact\_int(s,e,o,i,t) \ - \ Eff\_imp(s,e,o,i,t) \ si \ Eff\_imp(s,e,o,i,t) \ < \ Impact\_int(s,e,o,i,t) \\ 0 \qquad\qquad autrement \end{cases}$$

Tableau 62. Formule 22 : calcul de l'impact sur l'intégrité dans le cas des accès en écriture

Exemple : lorsqu'un sujet s_1 ayant un niveau de confidentialité *3,002* demande d'accéder en lecture à un objet o_1 ayant un niveau de confidentialité *4,01*, le calcul de l'impact se fait comme suit :

- *Impact_int(s_1, l, o_1, c, t) = 4,01/6,*
- *Impact(s_1, l, o_1, c, t) = Impact_int(s_1, l, o_1, c, t) – Eff_imp(s_1, l, o_1, c, t).*

Puisque *csl(s, t)*, qui est égale à *3,02*, appartient à *[3, 4[* et *col(o, t)*, qui est égale à *4,01*, appartient à *[4, 5[*, nous considérons les valeurs suivantes de la cellule *(]3, 4],]4, 5])* du *Tableau 54 :*

- *(m_1, l, 0,05, c, imp), (m_2, l, 0,1, c, imp), (m_3, l, 0,05, c, imp)* et *(m_4, l, 0,1, c, imp),*
- *Eff_imp(s_1, l, o_1, c, t) = 0,05 +0,1+0,05+0,1 = 0,3,*

- *Impact(s_1, l, o_1, c, t) = 4,01/6 – 0,3 = 0,668 – 0,3 = 0,368.*

8.5 Conclusion

Dans ce chapitre, nous avons défini des principes pour calculer l'impact des demandes d'accès. Ces principes se basent sur les niveaux de sécurité des sujets et des objets, et les flux d'informations. Nous avons présenté également des formules qui permettent de mesurer quantitativement l'impact tout en tenant compte de l'objectif de sécurité (confidentialité, intégrité) visé. De plus, nous avons intégré l'évaluation des *mesures de sécurité* qui permettent de réduire la valeur de l'impact intrinsèque.

Dans le chapitre suivant, nous utilisons les formules présentées dans ce chapitre afin de quantifier le risque des demandes d'accès.

Chapitre 9 : Évaluation et application de notre approche

9.1 Introduction

Dans cette thèse, nous avons développé les propriétés de notre approche pour *le calcul du risque* des requêtes d'accès. Cette approche permet de rendre plus flexibles les méthodes de contrôle d'accès traditionnel basées sur des décisions d'accès statiques et rigides, offre la possibilité de répondre aux besoins d'accès changeants des entreprises, et permet d'améliorer la qualité des décisions d'accès prises.

Dans ce chapitre, nous montrons que l'application de notre méthode de calcul du risque au modèle de contrôle d'accès *ABAC* [51] *(Voir la section 3.4 du chapitre 3)* est possible mais nécessite la modification de son processus de prise de décisions et l'ajout de nouveaux composants à son architecture.

Nous faisons également un ensemble de comparaisons pour montrer la pertinence et l'intérêt de chaque étape de notre approche. Nous comparons les valeurs obtenues par notre approche de calcul de la potentialité de la menace aux valeurs obtenues par la même approche lorsque les niveaux de confidentialité sont obtenus par le modèle du *High Water Mark (HWM) (Voir la section 3.2.1.4 du chapitre 3).* Cette comparaison nous permettra de démontrer l'importance de notre approche de calcul des niveaux de sécurité.

Nous comparons également les valeurs obtenues par notre approche de calcul du risque aux valeurs obtenues par notre approche de calcul du risque lorsque les niveaux de confidentialité sont obtenus par *HWM*. La comparaison des valeurs de risque obtenues dans ces deux cas nous permettra de confirmer les résultats obtenus par la comparaison précédente en montrant la capacité de notre approche à fournir des valeurs de risque évolutives.

Nous comparons aussi les valeurs d'impact obtenues en utilisant notre approche de calcul d'impact aux valeurs d'impact obtenues si les niveaux de sécurité sont statiques et aux valeurs obtenues par le modèle du *HWM* dans le cas de la confidentialité. Cela nous permet de montrer l'aspect évolutif des valeurs d'impact obtenues avec notre approche.

Nous calculons par la suite les valeurs du risque en intégrant les mesures de sécurité pour montrer que la considération de l'effet des mesures de sécurité permet d'avoir des valeurs plus réalistes conformément à la littérature d'analyse des risques.

Nous discutons également les différences entre notre approche de calcul du risque et celle de [60, 61] pour montrer les avantages de son utilisation.

Nous montrons également que notre approche permet de spécifier des politiques de contrôle d'accès que nous ne pouvons pas spécifier avec d'autres méthodes de contrôle d'accès. De plus, nous montrons qu'elle permet de choisir les sujets et les objets à inclure dans les tâches des flux de travail afin de minimiser les risques d'accès.

Nous montrons aussi via des graphiques qu'en suivant notre approche de calcul du risque, les valeurs du risque dépendent des valeurs de la potentialité de la menace et de l'impact qui dépendent des niveaux de sécurité dépendants à leur tour de l'historique des accès.

À la fin de ce chapitre, nous présentons un cas d'application de notre approche dans un système d'information hospitalier pour montrer ses spécificités et ses avantages.

Notons que dans ce chapitre, nous calculons les niveaux de confidentialité des sujets et des objets en considérant seulement les flux d'information reçus à partir des niveaux supérieurs ou égaux au niveau de l'entité qui reçoit les informations. De même, nous calculons les niveaux d'intégrité des sujets et des objets en considérant seulement les flux d'information reçus à partir des niveaux d'intégrité inférieurs ou égaux au niveau d'intégrité de l'entité qui reçoit les informations.

Ce chapitre est organisé comme suit : dans la section *2*, nous présentons l'application de notre approche de calcul du risque à *ABAC*. La section *3* présente une exploration des différents aspects de notre approche. Nous comparons notre approche aux approches de [60, 61] et nous montrons certaines de ses spécificités afin de montrer sa pertinence dans la section *4*. Dans la section *5*, nous montrons comment spécifier certaines politiques de contrôle d'accès et comment choisir les sujets et les objets qui représentent moins de risque à inclure dans les tâches des flux de travail, en utilisant notre approche. Dans la section *6*, nous montrons la dépendance entre les valeurs de potentialité de la menace et de l'impact, et les valeurs du risque. La section *7* présente des cas d'application de notre approche. La

section *8* récapitule les concepts présentés dans cette thèse. Nous concluons dans la section *9* par récapituler les caractéristiques de notre approche.

9.2 Application de notre approche à ABAC

Tenir compte des *niveaux de sécurité* changeants et des *mesures de sécurité* pour le calcul du risque implique une modification du processus de prise de décisions de *ABAC*. En effet, l'historique des accès sera transmis au calculateur des niveaux de sécurité. De plus, les niveaux de sécurité mis à jour et les évaluations de l'effet des mesures de sécurité mises en place, seront transmis au calculateur du risque. Les mesures de sécurité sont considérées comme des facteurs de l'environnement à prendre en considération pour calculer le risque avant de déterminer les décisions d'accès.

Dans le processus de prise de décision d'accès proposé par *ABAC* [51] que nous avons présenté dans la section *3.4* du chapitre *3*, lorsque le *point de décision de la politique* (*PDP*) reçoit une demande d'accès, il demande des informations supplémentaires au *point d'accès de la politique* (*PAP*) et au *point d'information de la politique* (*PIP*), pour prendre une décision. La méthode que nous proposons ajoute une nouvelle étape au cours de laquelle, le *PDP* demande la valeur du risque associée à une requête pour prendre une décision d'accès.

Le processus de prise de décision de notre approche est illustré dans la *Figure 40*. Au modèle *ABAC*, nous avons ajouté un calculateur des niveaux de sécurité, un calculateur du risque ainsi qu'un *point de politique du risque PRP*. Les nouveaux composants et flux que nous avons ajoutés sont représentés en pointillé.

Les différentes étapes à suivre pour déterminer une décision d'accès selon notre approche sont comme suit :

1. Le *PEP* reçoit une requête d'accès (étape *1*).
2. Le *PEP* transmet la requête d'accès au *PDP* (étape *2*).
3. Le *PDP* consulte la politique de sécurité (étape *3*).
4. Le *PDP* demande et reçoit les attributs relatifs à la demande d'accès à partir du *PIP* (étapes *4*, 5 et *6*).

5. Le *PDP* envoie une requête au *point de la politique du risque* (*PRP*) (étape *7*).
6. Le calculateur du risque reçoit les niveaux de sécurité des sujets et des objets (étape *8*).
7. Le calculateur du risque reçoit les valeurs de l'effet des mesures de sécurité (étape 9).
8. La valeur du risque associée à une demande d'accès est retournée au *PRP* puis au *PDP* (étapes *10* et *11*).
9. Sur la base de la valeur du risque, le *PDP* détermine une décision d'accès qui sera transmise au *PEP* qui l'applique (étape *12*).
10. Lorsque l'accès est autorisé, le *service d'obligations* envoie l'historique des accès au *calculateur des niveaux de sécurité* qui met à jour les *niveaux de sécurité* (étapes *13*, *14* et *15*).

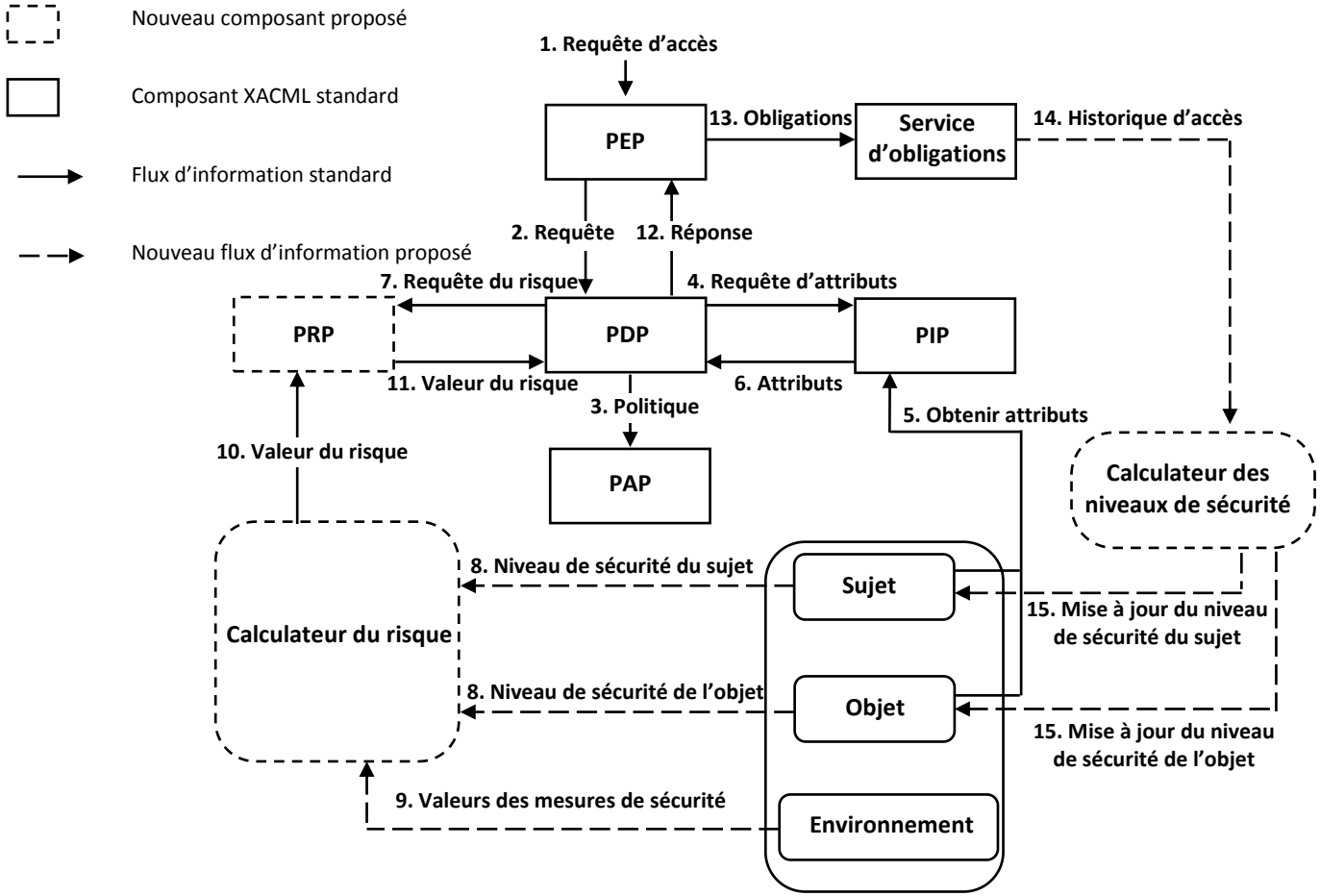


Figure 40. Flux du processus de la méthode de décision basée sur le risque

9.3 Évaluation de notre approche

Dans cette section, nous montrons la pertinence du choix des différentes étapes de notre approche. Cependant, nous ne montrerons pas les calculs détaillés afin d'alléger la présentation, étant donné que leurs principes ont été présentés dans les chapitres *6, 7* et *8*. Nous adopterons également les mêmes paramètres de ces chapitres.

Soit le tableau suivant qui représente les niveaux de confidentialité initiaux d'un ensemble de sujets et d'objets. Notons que dans les exemples cités dans cette section, nous considérons que seuls les accès cités ont été réalisés et nous supposons que l'effet des mesures de sécurité pour la réduction de la potentialité de la menace et de l'impact est nul. Cet effet sera pris en considération dans les exemples de la section *9.3.6*.

Entités	o_1	o_2	s_1	s_2	s_3	s_4	s_5	s_6	s_7
Niveaux de confidentialité initiaux	*3*	*4*	*3*	*3*	*3*	*2*	*4*	*4*	*4*

Tableau 63. Niveaux de confidentialité initiaux des sujets et des objets

9.3.1 Obtention de niveaux de sécurité différents en utilisant différentes approches de calcul des niveaux

Soient les deux exemples **Exemple 1** et **Exemple 2.**

9.3.1.1 Exemple 1

1. Jusqu'à l'instant t_1, l'objet o_1 qui a le niveau de confidentialité initial *3*, a été accédé en écriture par les *3* sujets s_1, s_2 et s_3 ayant le niveau de confidentialité initial *3*.
2. À l'instant t_2, le sujet s_4 ayant le niveau initial *2* a accédé en lecture à l'objet o_1.
3. Jusqu'à l'instant t_3, l'objet o_2 qui a le niveau initial *4* a été accédé en écriture par *3* sujets s_5, s_6 et s_7 ayant son propre niveau initial qui est *4*.
4. À l'instant t_4, le sujet s_4 demande d'accéder en lecture à l'objet o_2.

Les niveaux de confidentialité obtenus selon l'approche de calcul des niveaux de confidentialité *HWM* à l'instant t_4 sont comme suit :

1. $col(o_1, t_4) = col(o_1, t_1) = 3$.

2. $csl(s_4, t_4) = csl(s_4, t_2) = 3$.
3. $col(o_2, t_4) = col(o_2, t_3) = 4$.

Les niveaux de confidentialité obtenus selon notre approche de calcul des niveaux de confidentialité (*Voir la Formule 1 à la section 6.6.1 du chapitre 6*) à l'instant t_4 sont comme suit :

1. $col(o_1, t_4) = col(o_1, t_1) = 3{,}003$.
2. $csl(s_4, t_4) = csl(s_4, t_2) = 3{,}0031$.
3. $col(o_2, t_4) = col(o_2, t_3) = 4{,}03$.

9.3.1.2 Exemple 2

L'énoncé de l'**Exemple 2** est comme suit :

1. L'**Exemple 2** reprend l'**Exemple 1** mais suppose que jusqu'à l'instant t_3, l'objet o_2 qui a le niveau initial *4* n'a été accédé en écriture par aucun sujet.
2. À l'instant t_4, le sujet s_4 demande d'accéder en lecture à l'objet o_2.

Les niveaux de confidentialité obtenus selon l'approche de calcul des niveaux de confidentialité *HWM* à l'instant t_4 sont comme suit :

1. $col(o_1, t_4) = col(o_1, t_1) = 3$.
2. $csl(s_4, t_4) = csl(s_4, t_2) = 3$.
3. $col(o_2, t_4) = col(o_2, t_3) = 4$.

Les niveaux de confidentialité obtenus selon notre approche de calcul des niveaux de confidentialité (*Voir la Formule 1 à la section 6.6.1 du chapitre 6*) à l'instant t_4 sont comme suit :

1. $col(o_1, t_4) = col(o_1, t_1) = 3{,}003$.
2. $csl(s_4, t_4) = csl(s_4, t_2) = 3{,}0031$.
3. $col(o_2, t_4) = col(o_2, t_3) = 4$.

9.3.1.3 Comparaison des résultats obtenus dans l'Exemple 1 et l'Exemple 2

Nous remarquons que les valeurs des niveaux de confidentialité obtenues à l'instant t_4 par l'approche *HWM* dans l'**Exemple 1** et l'**Exemple 2** sont les mêmes alors que les valeurs des niveaux de confidentialité obtenues par notre approche, dans ces deux exemples, sont

différentes. Cela s'explique par le fait que notre approche permet de refléter l'historique des accès et par conséquent l'importance de la confidentialité des informations connues par les sujets et contenues dans les objets.

9.3.2 Obtention de valeurs de potentialité de menace différentes en utilisant les différentes approches d'évaluation des niveaux

Nous comparons maintenant les valeurs de potentialité de la menace obtenues en utilisant *HWM* comme approche pour l'évaluation des niveaux de confidentialité avec les valeurs de la potentialité de la menace obtenues en utilisant notre approche d'évaluation des niveaux.

Lorsque nous utilisons l'approche de calcul des niveaux de confidentialité *HWM* pour le calcul de la potentialité de la menace (*Voir* la *Formule 7 à la section 7.4.1.1 du chapitre 7*), à l'instant t_4, nous obtenons les valeurs suivantes :

Exemple 1 : $Menace\_int(s_4, l, o_2, c, t_4) = Menace(s_4, l, o_2, c, t_4) = 0{,}6571$.

Exemple 2 : $Menace\_int(s_4, l, o_2, c, t_4) = Menace(s_4, l, o_2, c, t_4) = 0{,}6571$.

Nous remarquons que nous obtenons la même valeur dans l'**Exemple 1** et l'**Exemple 2.**

Lorsque nous utilisons notre approche de calcul des niveaux de confidentialité pour le calcul de la potentialité de la menace (*Voir la Formule 7 à la section 7.4.1.1 du chapitre 7*), nous obtenons les valeurs suivantes :

Exemple 1 : $Menace\_int(s_4, l, o_2, c, t_4) = Menace(s_4, l, o_2, c, t_4) = 0{,}6613$.

Exemple 2 : $Menace\_int(s_4, l, o_2, c, t_4) = Menace(s_4, l, o_2, c, t_4) = 0{,}6570$.

Nous remarquons que la potentialité de la menace dans l'**Exemple 1** est supérieure à la potentialité de la menace dans l'**Exemple 2**. Cela s'explique essentiellement par l'augmentation du niveau de o_2 qui a été accédé en lecture dans l'**Exemple 1** et n'a pas été accédé en lecture dans l'**Exemple 2**. Les valeurs de la potentialité de la menace tiennent compte de l'historique des accès et des flux d'informations qui en découlent.

9.3.3 Obtention de niveaux d'impact différents en utilisant les différentes approches d'évaluation des niveaux

Dans cette section, nous comparons les valeurs de l'impact obtenues en utilisant *HWM* comme approche pour l'évaluation des niveaux de confidentialité et celles obtenues en utilisant notre approche d'évaluation des niveaux de confidentialité.

Lorsque nous utilisons l'approche de calcul des niveaux de confidentialité *HWM* pour le calcul de l'impact, sans considérer les mesures de sécurité réductrice de l'impact (*Voir la section 8.4 du chapitre 8*), nous obtenons les valeurs suivantes :

Exemple 1 : $Impact(s_4, l, o_2, c, t_4) = Impact\_int(s_4, l, o_2, c, t_4) = col(o_2, t_4) /6 = 4/6$.

Exemple 2 : $Impact(s_4, l, o_2, c, t_4) = Impact\_int(s_4, l, o_2, c, t_4) = col(o_2, t_4) /6 = 4/6$.

Nous remarquons qu'en utilisant l'approche *HWM*, les valeurs ne changent pas même si l'historique des accès de l'objet o_2 change.

Lorsque nous utilisons notre approche de calcul des niveaux de confidentialité pour le calcul de l'impact (*Voir la section 8.4 du chapitre 8*), nous obtenons les valeurs suivantes :

Exemple 1 : $Impact(s_4, l, o_2, t_4) = Impact\_int(s_4, l, o_2, c, t_4) = col(o_2, t_4) /6 = 4{,}003/6$.

Exemple 2 : $Impact(s_4, l, o_2, t_4) = Impact\_int(s_4, l, o_2, c, t_4) = col(o_2, t_4) /6 = 4/6$.

Nous remarquons que la valeur de l'impact dans l'**Exemple 1** est supérieure à la valeur de l'impact dans l'**Exemple 2**. En effet, les valeurs de l'impact obtenues en utilisant notre approche considèrent les flux d'informations reçus par l'objet o_2 jusqu'à l'instant t_4.

9.3.4 Obtention de valeurs de risque différentes en utilisant les différentes approches d'évaluation des niveaux

Dans cette section, nous comparons les valeurs de risque obtenues en utilisant *HWM* comme approche pour l'évaluation des niveaux de confidentialité et les valeurs de risque obtenues en utilisant notre approche d'évaluation des niveaux de confidentialité.

Les valeurs du risque se calculent comme suit : $Risque(s_4, l, o_2, c, t_4) = Menace(s_4, l, o_2, c, t) \times Impact(s_4, l, o_2, c, t)$. Lorsque nous utilisons l'approche *HWM* pour le calcul des

niveaux de confidentialité et notre approche pour le calcul de la potentialité de la menace, (*Voir la Formule 7 à la section 7.4.1.1 du chapitre 7*) nous obtenons les valeurs de risque suivantes :

Exemple 1 : $Risque(s_4, l, o_2, c, t_4) = Menace(s_4, l, o_2, c, t_4) \times Impact(s_4, l, o_2, c, t_4) = 0,6571 \times 4/6 = 0,43806.$

Exemple 2 : $Risque(s_4, l, o_2, c, t_4) = Menace(s_4, l, o_2, c, t_4) \times Impact(s_4, l, o_2, c, t_4) = 0,6571 \times 4/6 = 0,43806.$

Nous remarquons qu'en utilisant l'approche *HWM*, les valeurs du risque obtenues dans les deux exemples sont égales, même si les historiques d'accès ne sont pas les mêmes. Lorsque nous utilisons notre approche pour le calcul des niveaux de confidentialité et notre approche pour le calcul de la potentialité de la menace, nous obtenons les valeurs de risque suivantes :

Exemple 1 : $Risque(s_4, l, o_2, c, t_4) = 0,6613 \times 4,003/6 = 0,4411$.

Exemple 2 : $Risque(s_4, l, o_2, c, t_4) = 0,6570 \times 4/6 = 0,438.$

En utilisant notre approche pour le calcul du risque, les valeurs du risque ne sont pas les mêmes puisque notre approche tient compte de l'historique d'accès. Tenir compte de l'historique des accès permettrait d'assurer davantage la confidentialité en permettant l'interdiction des accès les plus risquées.

9.3.5 Obtention de valeurs de risque différentes en intégrant les mesures de sécurité

Selon notre approche pour le calcul du risque, le risque d'une requête de sécurité se calcule comme suit : $Risque(s_4, l, o_2, c, t_4) = (Menace\_int(s_4, l, o_2, c, t_4) - Eff\_pot(s_4, l, o_2, c, t_4)) \times (Impact\_int(s_4, l, o_2, c, t_4) - Eff\_imp(s_4, l, o_2, c, t_4))$.

Soient les trois cas suivants qui considèrent les accès cités dans l'**Exemple 1.**

Cas 1

L'effet des mesures de sécurité pour réduire la potentialité de la menace et l'effet des mesures de sécurité pour réduire l'impact sont nuls. Ainsi, la valeur du risque obtenue par notre approche est la suivante : $Risque(s_4, l, o_2, c, t_4) = 0,6613 \times (4,003/6) = 0,4411$.

Cas 2

L'effet des mesures de sécurité pour réduire la potentialité de la menace est égale à *0,5* et l'effet des mesures de sécurité pour réduire l'impact est égale à *0,25*. Ainsi la valeur du risque obtenue par notre approche est la suivante : $Risque(s_4, l, o_2, c, t_4) = (0,6613 - 0,5) \times (4,003/6 - 0,25) = 0,0672$.

Cas 3

L'effet des mesures de sécurité pour réduire la potentialité de la menace est égale à *0,1* et l'effet des mesures de sécurité pour réduire l'impact est égale à *0,25*. Ainsi la valeur du risque obtenue par notre approche est la suivante : $Risque(s_4, l, o_2, c, t_4) = (0,6613 - 0,1) \times (4,003/6 - 0,25) = 0,2341$.

Nous remarquons que la considération de l'effet des mesures de sécurité réductrices de la potentialité de la menace et de l'impact permet de changer les valeurs du risque. Cela permet d'obtenir des évaluations plus réalistes en conformité avec la littérature de l'analyse des risques.

9.4 Comparaison de notre approche avec l'approche présentée dans [60, 61]

Dans le cas d'une requête où un sujet demande d'accéder en lecture à un objet ayant un niveau d'intégrité inférieur lorsque l'objectif d'intégrité est visé et dans le cas d'une requête où un sujet demande d'accéder en écriture à un objet ayant un niveau de confidentialité inférieur lorsque l'objectif de confidentialité est visé, les valeurs du risque obtenues par notre approche sont différentes des valeurs obtenues par l'approche présentée dans les articles [60, 61].

9.4.1 Cas des accès en lecture lorsque l'objectif d'intégrité est visé

Soit l'exemple suivant : à l'instant t_1, le sujet s_1 ayant le niveau d'intégrité *4* demande d'accéder en lecture à l'objet o_2 ayant le niveau d'intégrité *2*. En adoptant l'approche de l'article [61], le risque de la requête est égal à *0* alors qu'en adoptant notre approche le risque de la requête est supérieur à *0*. Cela signifie que des demandes d'accès acceptées par l'approche de [61] seront refusées par notre approche pour préserver l'intégrité. Rappelons que le passage de l'information d'un niveau inférieur à un niveau supérieur dans le cas de l'intégrité diminue l'intégrité de l'information au niveau supérieur. Cela justifie la valeur positive du risque obtenue en utilisant notre approche.

9.4.2 Cas des accès en écriture lorsque l'objectif de confidentialité est visé

Soit l'exemple suivant : à l'instant t_1, le sujet s_1 ayant le niveau de confidentialité *4* demande d'accéder en écriture à l'objet o_2 ayant le niveau de confidentialité *2*. En adoptant l'approche de l'article [61], le risque de la requête est égale à *0* alors qu'en adoptant notre approche le risque de la requête est supérieur à *0*. Cela signifie que des demandes d'accès acceptés par l'approche de [61] seront refusés par notre approche pour préserver la confidentialité. Rappelons que le passage de l'information d'un niveau supérieur à un niveau inférieur dans le cas de la confidentialité représente un risque sur la confidentialité de l'information. Cela justifie la valeur positive du risque obtenue en utilisant notre approche.

9.5 Spécification des politiques de contrôle d'accès et priorisation des tâches des flux de travail

Dans cette section, nous montrons qu'en utilisant notre approche, il est possible de spécifier des politiques de contrôle d'accès spécifiques qui permettent de tenir compte des flux d'informations. De plus, nous montrons que cette approche permet de choisir les sujets et les objets qui représentent moins de risque pour les inclure dans les tâches des flux de travail.

9.5.1 Spécification des politiques de contrôle d'accès

Notre approche permet de spécifier des politiques de contrôle d'accès que nous ne pouvons pas spécifier avec les modèles de contrôle d'accès traditionnels. Soit la politique suivante : un sujet ayant un niveau de confidentialité inférieur ou égale à *3* n'a pas le droit de connaître le contenu de deux entités ayant le niveau de confidentialité *5* en un seul accès. Pour appliquer cette politique nous devons déterminer la valeur maximale du risque acceptable. Dans cet exemple, les valeurs du risque acceptable doivent être inférieures à la valeur du risque lorsqu'un objet ayant un niveau *3* demande d'accéder à un objet ayant un niveau de confidentialité *5,19999* qui est le niveau de confidentialité maximal d'un objet ayant reçu des flux d'information de deux entités ayant le niveau *5*. Le niveau de confidentialité d'un objet ayant reçu des flux d'informations de deux entités ayant le niveau *5* est égale à *5,1*. Selon la *Formule 7* (*Voir la section 7.4 du chapitre 7*), la valeur maximale du risque acceptable est calculée comme suit : $(5 \times 5{,}1999 + 3)/(35) \times (5\ ,\ 1999)/(6\ ) = 0{,}718$. Ainsi les requêtes d'accès des sujets ayant un niveau de confidentialité inférieur ou égale à *3* seraient acceptées lorsque $Risque(s, a, o, c, t) \leq 0{,}718$.

Notre approche permet de spécifier des politiques que nous ne pouvons pas spécifier en adoptant des approches basées sur des niveaux statiques ou sur *HWM*. En utilisant une approche statique ou l'approche *HWM*, il n'est pas possible de comptabiliser le nombre des flux d'informations reçus.

9.5.2 Priorisation des tâches de flux de travail

Dans ce qui suit, nous montrons comment notre approche de calcul du risque nous permet de choisir les sujets et les objets qui représentent moins de risque pour les inclure dans les tâches des flux de travail. Cela n'est pas possible avec d'autres approches de contrôle d'accès. Dans cette sous-section, nous considérons les niveaux de confidentialité initiaux d'un ensemble de sujets et d'objets, présentés dans le *Tableau 64.* Nous considérons également que l'effet des mesures de sécurité est nul.

Entités	o_1	o_2	o_3	o_4	o_5	o_6	o_7	o_8	s_1	s_2	s_3	s_4	s_5
Niveaux de confidentialité initiaux	*3*	*4*	*3*	*3*	*3*	*2*	*4*	*1*	*4*	*4*	*3*	*3*	*2*

Tableau 64. Niveaux de confidentialité initiaux

Soient les flux de travail suivants :

Le *Flux de travail 1* représenté par la *Figure 41* est décrit comme suit : le sujet s_1 lit les objets o_1, o_2 et o_3 puis écrit dans l'objet o_4.

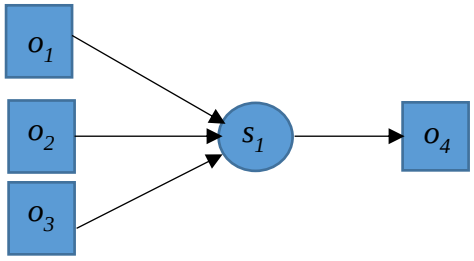


Figure 41. Flux de travail 1

Le *Flux de travail 2* représenté par la *Figure 42* est décrit comme suit : le sujet s_2 lit les objets o_5 et o_6 puis écrit dans l'objet o_7.

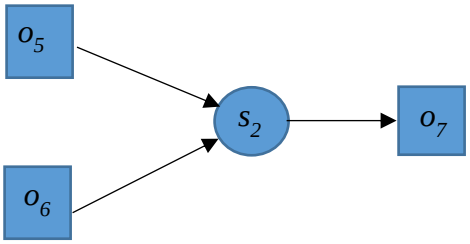


Figure 42. Flux de travail 2

Le *Flux de travail 3* consiste à autoriser le sujet s_3 à lire le contenu d'un objet parmi les objets o_4 et o_7. Quel est l'objet dont l'intégration dans le *Flux de travail 3* est la moins risquée ?

La *Figure 43* représente le choix d'objet le moins risqué. En effet, l'objet o_7 est l'objet dont l'intégration dans le flux de travail est la moins risquée puisque o_4 a reçu deux flux d'informations à partir du niveau *4* alors que l'objet o_7 a reçu un flux du même niveau *4*. L'objet o_7 a un niveau de confidentialité inférieur au niveau de confidentialité de o_4. Ainsi le risque d'accès de s_3 à o_7 serait moins élevé que l'accès de s_3 à o_4.

1. $col(o_7, t) < col(o_4, t)$.

2. *Menace(s_3, l, o_7, c, t) < Menace(s_3, l, o_4, c, t).*
3. *Impact(s_3, l, o_7, c, t) < Impact(s_3, l, o_4, c, t).*

D'après *1*, *2* et *3*, *Risque(s_3, l, o_7, c, t) < Risque(s_3, l, o_4, c, t).*

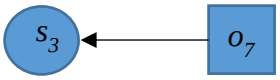


Figure 43. Flux de travail 3

Le *Flux de travail 4* consiste à autoriser un sujet parmi les sujets s_4 et s_5 à écrire dans l'objet o_8 ayant le niveau de confidentialité *1*. Quel est le sujet dont l'intégration dans le *Flux de travail 4* est la moins risquée ?

Le sujet s_5 est le sujet dont l'intégration dans le *Flux de travail 4* est la moins risquée puisque le sujet s_5 a un niveau de confidentialité inférieur au niveau de confidentialité de s_4. Ainsi le risque d'accès en écriture de s_5 à o_8 serait moins élevé que le risque d'accès de s_4 à o_8.

1. *csl(s_5, t) < csl(s_4, t).*
2. *Menace(s_5, e, o_8, c, t) < Menace(s_4, e, o_8, c, t).*
3. *Impact(s_5, e, o_8, c, t) < Impact(s_4, e, o_8, c, t).*

D'après *1*, *2* et *3*, *Risque(s_5, e, o_8, c, t) < Risque(s_4, e, o_8, c, t).*

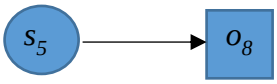


Figure 44. Flux de travail 4

D'après les exemples cités dans cette sous-section, nous pouvons voir qu'en utilisant notre approche qualitative, nous sommes capables de sélectionner les sujets et les objets dont l'intégration dans les différentes tâches d'un flux de travail représente moins de risque. Notre approche quantitative peut confirmer les choix basés sur notre méthode qualitative.

9.6 Dépendance entre les niveaux de sécurité, la potentialité de la menace, l'impact et le risque

Soit l'exemple suivant :

1. À l'instant *1*, l'objet o_2 qui a le niveau de confidentialité initial *4* est accédé en lecture.
2. À l'instant *2*, l'objet o_2 a été accédé en écriture par un sujet ayant un niveau initial de confidentialité *5* et qui a reçu *3* autres flux d'informations du niveau *5*.
3. À l'instant *3*, l'objet o_2 a été accédé en écriture par un autre sujet ayant un niveau initial de confidentialité 5 et qui a reçu un flux d'informations du niveau *5*.
4. À l'instant *4*, l'objet o_2 a été accédé en écriture par un autre sujet ayant le niveau initial de confidentialité *5* et qui a reçu un flux d'informations du niveau 5.
5. À l'instant *5*, l'objet o_2 a été accédé en écriture par un autre sujet ayant le niveau initial de confidentialité *5* et qui n'a pas reçu de flux d'informations.

D'après le *Tableau 66* et la *Figure 45* qui montrent l'évolution des niveaux de confidentialité du niveau de l'objet o_2, nous remarquons ce qui suit :

- Les valeurs obtenues par notre approche (*Voir la Formule 2 à la section 6.6.2 du chapitre 6*) continuent à augmenter dans le temps.
- Les valeurs obtenues par *HWM* augmentent puis deviennent statiques.
- Les valeurs obtenues par une approche statique n'évoluent pas dans le temps.

Instants / ***Approches***	*0*	*1*	*2*	*3*	*4*	*5*
Notre approche	*4*	*4*	*5,31*	*5,51*	*5,71*	*5,81*
HWM	*4*	*4*	*5*	*5*	*5*	*5*
Statique	*4*	*4*	*4*	*4*	*4*	*4*

Tableau 65. Évolution du niveau de confidentialité de l'objet o_2 dans le temps selon les approches

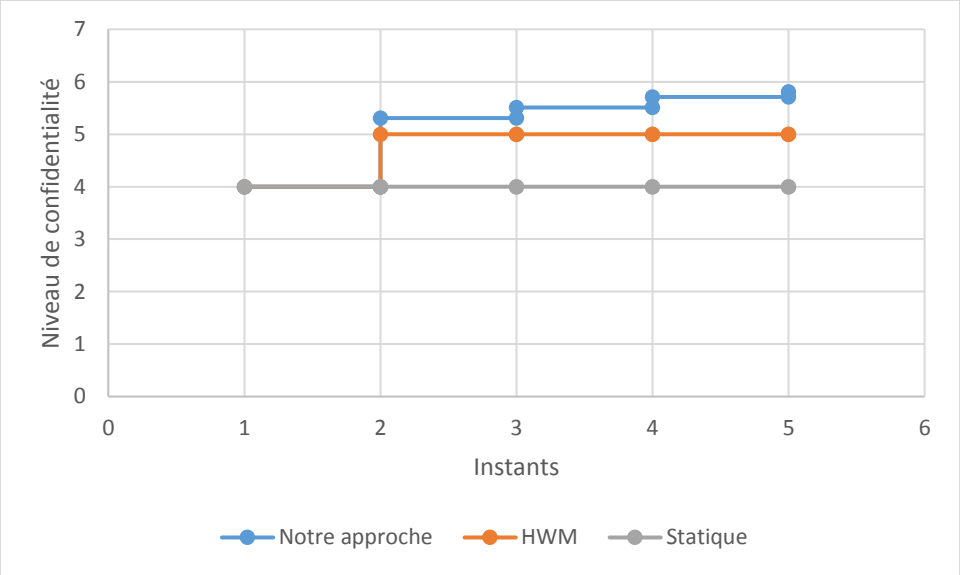


Figure 45. Évolution du niveau de confidentialité de o_2 dans le temps selon les approches à partir de l'instant *1*

D'après le *Tableau 67 et* la *Figure 46* qui montrent l'évolution des potentialités de la menace de l'accès d'un sujet ayant un niveau de confidentialité *2* à l'objet o_2 aux instants *1*, *2*, *3*, *4* et *5*, nous remarquons ce qui suit :

- Les valeurs de la potentialité de la menace obtenues par notre approche augmentent dans le temps (comme le niveau de l'objet).
- Les valeurs de la potentialité de la menace obtenues par *HWM* augmentent puis deviennent statiques (comme le niveau de l'objet).
- Les valeurs de la potentialité de la menace obtenues par une approche statique n'évoluent pas dans le temps (comme le niveau de l'objet).

Instants / ***Approches***	*1*	*2*	*3*	*4*	*5*
Notre approche	*0,685*	*0,872*	*0,901*	*0,93*	*0,944*
HWM	*0,685*	*0,828*	*0,828*	*0,828*	*0,828*
Statique	*0,685*	*0,685*	*0,685*	*0,685*	*0,685*

Tableau 66. Évolution de la potentialité intrinsèque de la menace dans le temps selon les approches

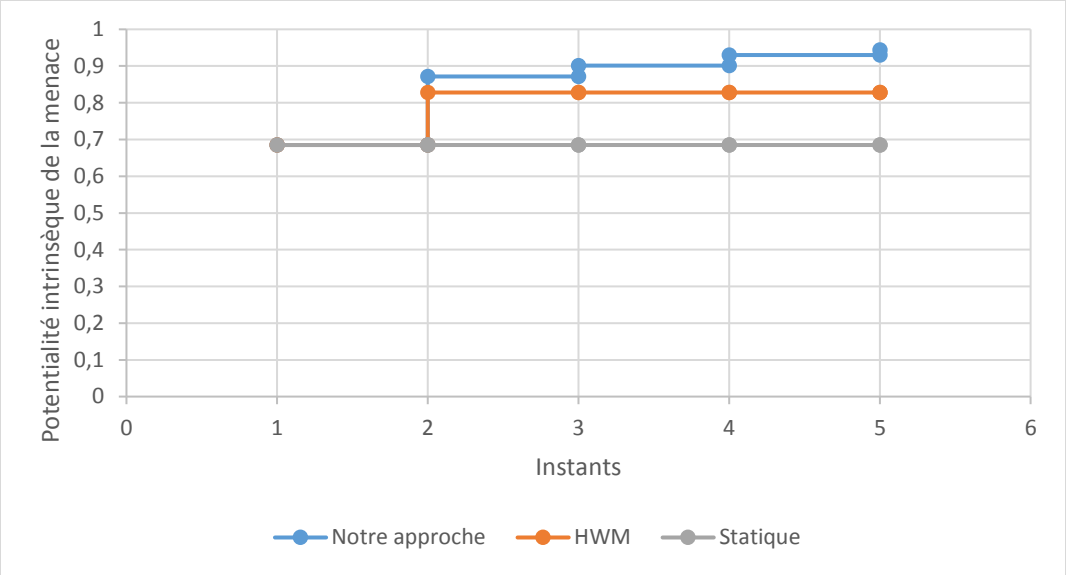


Figure 46. Évolution de la potentialité intrinsèque de la menace dans le temps selon les approches

D'après le *Tableau 68* et la *Figure 47* qui montrent l'évolution des impacts de l'accès d'un sujet ayant un niveau *2* à l'objet o_2 aux instants *1*, *2*, *3*, *4* et *5*, nous remarquons ce qui suit :

- Les valeurs de l'impact obtenues par notre approche (*Voir la section 8.4 du chapitre 8*) augmentent dans le temps (comme le niveau de l'objet).
- Les valeurs de l'impact obtenues par *HWM* augmentent puis deviennent statiques (comme le niveau de l'objet).
- Les valeurs de l'impact obtenues par une approche statique sont statiques (comme le niveau de l'objet).

Instants / ***Approches***	*1*	*2*	*3*	*4*	*5*
Notre approche	*0,66*	*0,885*	*0,918*	*0,951*	*0,968*
HWM	*0,66*	*0,833*	*0,833*	*0,833*	*0,833*
Statique	*0,66*	*0,66*	*0,66*	*0,66*	*0,66*

Tableau 67. Évolution des valeurs de l'impact dans le temps selon les approches

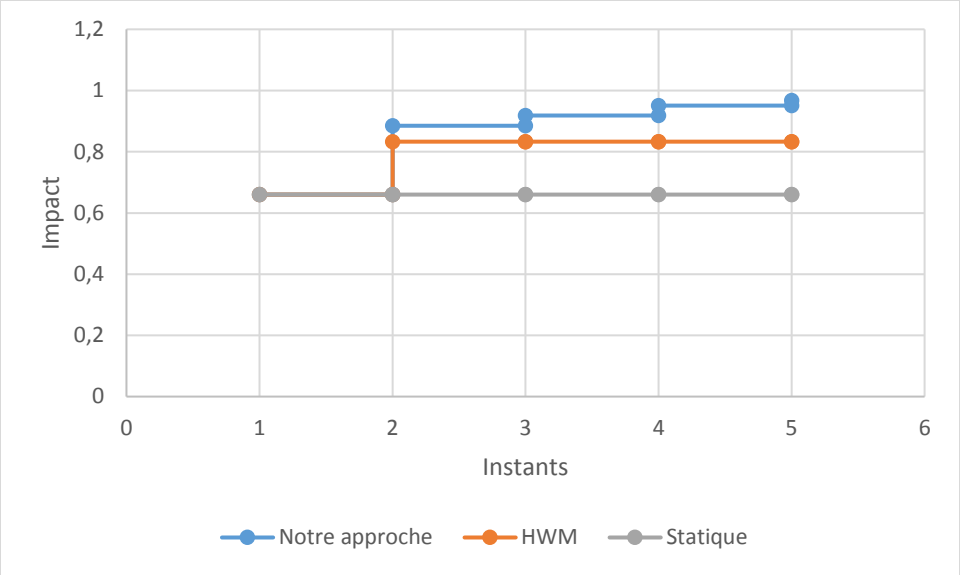


Figure 47. Évolution des valeurs de l'impact dans le temps selon les approches

D'après le *Tableau 69* et la *Figure 48* qui montrent l'évolution des risques de l'accès d'un sujet ayant un niveau *2* à l'objet o_2 aux instants *1*, *2*, *3*, *4* et *5*, nous remarquons ce qui suit :

- Les valeurs du risque obtenues par notre approche augmentent dans le temps (comme le niveau de l'objet).
- Les valeurs du risque obtenues par *HWM* augmentent puis deviennent statiques (comme le niveau de l'objet).
- Les valeurs du risque obtenues par une approche statique sont statiques (comme le niveau de l'objet).

Instants / ***Approche***	*1*	*2*	*3*	*4*	*5*
Notre approche	*0,452*	*0,771*	*0,827*	*0,884*	*0,913*
HWM	*0,452*	*0,689*	*0,689*	*0,689*	*0,689*
Statique	*0,452*	*0,452*	*0,452*	*0,452*	*0,452*

Tableau 68. Évolution des niveaux de risque

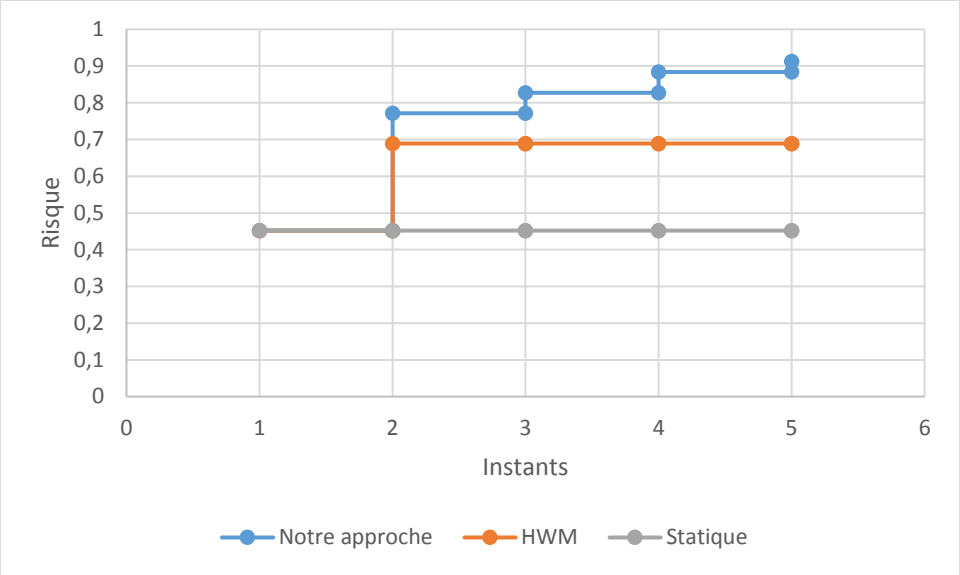


Figure 48. Évolution du risque dans le temps selon les approches

9.7 Cas d'application

Dans cette section, nous présentons des cas d'application pour montrer l'intérêt pratique de notre approche. Pour cela, nous considérons un système d'information hospitalier composé de ressources humaines, logicielles et matérielles destinées à assurer la communication de l'information entre tous les intervenants à l'hôpital. Dans nos exemples suivants, nous nous limitons aux intervenants suivants : les patients, les médecins et les infirmières. Ce système d'information hospitalier est composé d'un réseau local informatique et de connexions à des sites distants. Un système de contrôle d'accès gère l'accès aux dossiers des patients.

9.7.1 Mesures de sécurité

Les mesures de sécurité qui peuvent être mises en place sont les suivantes :

1. L'activation de la journalisation des accès (mesure m_1).
2. L'authentification forte des sujets avant l'authorisation des accès (mesure m_2).
3. La signature d'une politique sur l'utilisation des actifs informationnels par tous les employés (mesure m_3). Cette politique détermine les sanctions à appliquer dans le cas de la violation de la politique de sécurité.

4. Le transfert des données qui se fait par un réseau privé virtuel crypté ou à partir du site local (mesure m_4).
5. La restauration des informations avec des copies de sauvegarde (mesure m_5).

Le *Tableau 70* et le *Tableau 71* représentent respectivement les valeurs de la réduction de la potentialité de la menace et de l'impact en fonction des niveaux de sécurité des sujets et des objets et l'objectif de sécurité visé. Dans ce qui suit, nous présentons deux cas pour illustrer l'utilité de notre approche de calcul du risque.

Niveau de confidentialité des sujets	***Niveau de confidentialité des objets***				
	[1, 2[	*[2, 3[*	*[3, 4[*	*[4, 5[*	*[5, 6[*
[1, 2[	*(m_1, l, 0,075, c, pot)* *(m_2, l, 0,15, c, pot)* *(m_3, l, 0,05, c, pot)* *(m_4, l, 0,1, c, pot)*	*(m_1, l, 0,075, c, pot)* *(m_2, l, 0,15, c, pot)* *(m_3, l, 0,05, c, pot)* *(m_4, l, 0,1, c, pot)*	*(m_1, l, 0,05, c, pot)* *(m_2, l, 0,1, c, pot)* *(m_3, l, 0,05, c, pot)* *(m_4, l, 0,1, c, pot)*	*(m_1, l, 0,04, c, pot)* *(m_2, l, 0,05, c, pot)* *(m_3, l, 0,04, c, pot)* *(m_4, l, 0,1, c, pot)*	*(m_1, l, 0,03, c, pot)* *(m_2, l, 0,01, c, pot)* *(m_3, l, 0,03, c, pot)* *(m_4, l, 0,1, c, pot)*
[2, 3[		*(m_1, l, 0,07, c, pot)* *(m_2, l, 0,1, c, pot)* *(m_3, l, 0,05, c, pot)* *(m_4, l, 0,1, c, pot)*	*(m_1, l, 0,05, c, pot)* *(m_2, l, 0,1, c, pot)* *(m_3, l, 0,05, c, pot)* *(m_4, l, 0,1, c, pot)*	*(m_1, l, 0,03, c, pot)* *(m_2, l, 0,07, c, pot)* *(m_3, l, 0,05, c, pot)* *(m_4, l, 0,05, c, pot)*	*(m_1, l, 0,02, c, pot)* *(m_2, l, 0,05, c, pot)* *(m_3, l, 0,03, c, pot)* *(m_4, l, 0,03, c, pot)*
[3, 4[			*(m_1, l, 0,05, c, pot)* *(m_2, l, 0,1, c, pot)* *(m_3, l, 0,05, c, pot)* *(m_4, l, 0,1, c, pot)*	*(m_1, l, 0,05, c, pot)* *(m_2, l, 0,1, c, pot)* *(m_3, l, 0,05, c, pot)* *(m_4, l, 0,1, c, pot)*	*(m_1, l, 0,05, c, pot)* *(m_2, l, 0,1, c, pot)* *(m_3, l, 0,05, c, pot)* *(m_4, l, 0,1, c, pot)*
[4, 5[				*(m_1, l, 0,05, c, pot)* *(m_2, l, 0,1, c, pot)*	*(m_1, l, 0,05, c, pot)* *(m_2, l, 0,1, c, pot)*

				(m_3, l, 0,05, c, pot) *(m_4, l, 0,1, c, pot)*	*(m_3, l, 0,05, c, pot)* *(m_4, l, 0,1, c, pot)*
[5, 6[					*(m_1, l, 0,05, c, pot)* *(m_2, l, 0,1, c, pot)* *(m_3, l, 0,05, c, pot)* *(m_4, l, 0,1, c, pot)*

Tableau 69. Effet des mesures de sécurité réductrices de la potentialité de la menace

Niveau d'intégrité des sujets	***Niveau d'intégrité des objets***				
	]4,5]	*]3,4]*	*]2,3]*	*]1,2]*	*]0,1]*
]4,5]	*(m_5, l, 0,25, i, imp)*	*(m_5, l, 0,25, i, imp)*	*(m_5, l, 0,25, i, imp)*	*(m_5, l, 0,25, i, imp)*	*(m_5, l, 0,25, i, imp)*
]3,4]		*(m_5, l, 0,25, i, imp)*	*(m_5, l, 0,25, i, imp)*	*(m_5, l, 0,25, i, imp)*	*(m_5, l, 0,25, i, imp)*
]2,3]			*(m_5, l, 0,25, i, imp)*	*(m_5, l, 0,25, i, imp)*	*(m_5, l, 0,3, i, imp)*
]1,2]				*(m_5, l, 0,25, i, imp)*	*(m_5, l, 0,3, i, imp)*
]0,1]					*(m_5, l, 0,3, i, imp)*

Tableau 70. Effet des mesures de sécurité réductrices de l'impact

9.7.2 Cas 1

Dans cet exemple, nous calculons le risque des demandes d'accès de trois médecins à un instant *t*, en suivant toutes les étapes de notre approche de calcul du risque. *$Médecin_1$*, *$Médecin_2$* et *$Médecin_3$* ont des niveaux initiaux de confidentialité égaux à *3*. L'historique des accès des médecins est comme suit :

1. *$Médecin_1$ et $Médecin_3$* n'ont accédé à *aucun fichier*,
2. *$Médecin_2$* a accédé à *2* fichiers F_{p1} et F_{p2} ayant le niveau de confidentialité *4*.

Une situation d'urgence nécessite la consultation à l'instant *t* du fichier F_p d'un patient qui est classé *Top secret* ($col(F_p, t) = 5$). Ce fichier n'a été accédé en écriture par aucun médecin. Aucun des médecins ayant l'habilitation pour le lire n'est présent. Les trois médecins $Médecin_1$, $Médecin_2$ et $Médecin_3$ seraient capables de le lire comme suit :

1. $Médecin_1$ peut se connecter à partir du *site local* à l'instant *t*,
2. $Médecin_2$ peut se connecter à partir du *site distant 1* via un réseau privé virtuel crypté à l'instant *t*,
3. $Médecin_3$ peut se connecter à partir du *site distant 2* via un réseau privé virtuel non crypté à l'instant *t*,
4. les mesures m_1, m_2 et m_3 sont mises en place pour tous les médecins.

Dans ce qui suit, nous répondons à un ensemble de questions en utilisant notre approche de calcul du risque.

Question 1

La première question à laquelle nous répondons est la suivante : lequel des médecins devrait être autorisé à lire le contenu du fichier F_p ?

Le calcul du risque des demandes d'accès selon notre approche consiste à utiliser les valeurs obtenues dans les étapes qui suivent.

À l'instant *t* de la demande d'accès, les niveaux de confidentialité obtenus (*Voir la Formule 1 à la section 6.6.1 du chapitre 6*) sont comme suit :

- $csl(Médecin_1, t) = 3$.
- $csl(Médecin_2, t) = 4{,}011$.
- $csl(Médecin_3, t) = 3$.

Les valeurs de la potentialité intrinsèque de la menace pour chaque demandeur d'accès (*Voir la Formule 7 à la section 7.4.1.1 du chapitre 7*) sont comme suit :

- $Menace\_int(Médecin_1, l, F_p, c, t) = 0{,}8$.
- $Menace\_int(Médecin_2, l, F_p, c, t) = 0{,}771$.
- $Menace\_int(Médecin_3, l, F_p, c, t) = 0{,}8$.

L'effet des mesures de la réduction de la potentialité de la menace à considérer pour la demande d'accès de $Médecin_1$:

$Eff\_pot(Médecin_1, l, F_p, c, t) = 0,30.$

L'effet des mesures de la réduction de la potentialité de la menace à considérer pour la demande d'accès de $Médecin_2$:

$Eff\_pot(Médecin_2, l, F_p, c, t) = 0,30.$

L'effet des mesures de la réduction de la potentialité de la menace à considérer pour la demande d'accès de $Médecin_3$:

$Eff\_pot(Médecin_3, l, F_p, c, t) = 0,20$ ($0,2 = 0,3 - 0,1$, étant donnée que l'accés se fait à distance via un réseau non crypté).

La potentialité de la menace pour chaque demande d'accès (*Voir la section 7.4 du chapitre 7*) est calculée comme suit :

- $Menace(Médecin_1, l, F_p, c, t) = Menace\_int(Médecin_1, l, F_p, c, t) – Eff\_pot(Médecin_1, l, F_p, c, t) = 0,8 - 0,3 = 0,5.$
- $Menace(Médecin_2, l, F_p, c, t) = Menace\_int(Médecin_2, l, F_p, c, t) – Eff\_pot(Médecin_2, l, F_p, c, t) = 0,771 - 0,3 = 0,471.$
- $Menace(Médecin_3, l, F_p, c, t) = Menace\_int(Médecin_3, l, F_p, c, t) – Eff\_pot(Médecin_3, l, F_p, c, t) = 0,8 - 0,2 = 0,6.$

Les valeurs d'impact intrinsèque des demandes d'accès des trois médecins sont obtenues comme suit :

- $Impact\_int(Médecin_1, l, F_p, c, t) = 5/6.$
- $Impact\_int(Médecin_2, l, F_p, c, t) = 5/6.$
- $Impact\_int(Médecin_3, l, F_p, c, t) = 5/6.$

Les effets des mesures de la réduction de l'impact à considérer pour les demandes d'accès des trois médecins sont comme suit :

- $Eff\_imp(Médecin_1, l, F_p, c, t) = 0.$
- $Eff\_imp(Médecin_2, l, F_p, c, t = 0.$
- $Eff\_imp(Médecin_3, l, F_p, c, t) = 0.$

Les valeurs d'impact des demandes d'accès des trois médecins sont calculées comme suit :

- $Impact(Médecin_1, l, F_p, c, t) = Impact\_int(Médecin_1, F_p, l, c, t) - Eff\_imp(Médecin_1, l, F_p, c, t) = 5/6.$
- $Impact(Médecin_2, l, F_p, c, t) = Impact\_int(Médecin_2, F_p, l, c, t) - Eff\_imp(Médecin_2, l, F_p, c, t) = 5/6.$
- $Impact(Médecin_3, l, F_p, c, t) = Impact\_int(Médecin_3, F_p, l, c, t) - Eff\_imp(Médecin_3, l, F_p, c, t) = 5/6.$

Les valeurs de risque des demandes d'accès des trois médecins sont calculées comme suit :

- $Risque(Médecin_1, l, F_p, c, t) = Menace(Médecin_1, l, F_p, c, t) \times Impact(Médecin_1, l, F_p, c, t) = 0,5 \times (5/6) = 0,416.$
- $Risque(Médecin_2, l, F_p, c, t) = Menace(Médecin_2, l, F_p, c, t) \times Impact(Médecin_2, l, F_p, c, t) = 0,471 \times (5/6) = 0,3925.$
- $Risque(Médecin_3, l, F_p, c, t) = Menace(Médecin_3, l, F_p, c, t) \times Impact(Médecin_3, l, F_p, c, t) = 0,6 \times (5/6) = 0,5.$

D'après ce qui précède, l'accès en lecture de $Médecin_2$ au fichier F_p est moins risqué que l'accès de $Médecin_1$ et $Médecin_3$ en lecture au même fichier F_p $(0,3925 < 0,416 < 0,5).$

Question 2

Supposons que le réseau virtuel privé crypté n'est pas fonctionnel et seul l'accès par le réseau privé virtuel non crypté est possible, lequel des médecins devrait être autorisé à lire le contenu de ce fichier dans ce cas ?

La nouvelle valeur du risque de $Médecin_2$ lorsque le réseau virtuel crypté n'est plus fonctionnel est calculée comme suit :

- $Eff\_pot(Médecin_2, l, F_p, c, t) = 0,2.$
- $Menace(Médecin_2, l, F_p, c, t) = Menace\_int(Médecin_2, l, F_p, c, t) - Eff\_pot(Médecin_2, l, F_p, c, t) = 0,771 - 0,2 = 0,571.$
- $Risque(Médecin_2, l, Fp, c, t) = Menace(Médecin_2, l, F_p, c, t) \times Impact(Médecin_2, l, F_p, c, t) = 0,571 \times (5/6) = 0,475.$

D'après ce qui précède, l'accès de $Médecin_1$ est moins risqué que les accès des autres médecins. L'accès de $Médecin_2$ devient plus risqué que l'accès de $Médecin_1$ *(0,416 < 0,475 < 0,5)*.

Question 3

Est-ce qu'un médecin autorisé à accéder à ce fichier à un instant donné *t*, le serait à un instant ultérieur *t'', avec* $t < t' < t''$, sachant que $Médecin_1$ et $Médecin_2$ n'ont accédé à aucun fichier à l'instant *t'*, et que $Médecin_3$ a accédé à *3* fichiers ayant le niveau de confidentialité *4* à l'instant *t'* ?

D'après les accès cités dans ce qui précède, nous constatons que les niveaux de confidentialité de $Médecin_1$ et $Médecin_2$ n'ont pas changé. Conséquemment les valeurs de risque de leurs accès ne vont pas changer. Pour cela nous calculons la nouvelle valeur du risque d'accès de $Médecin_3$, en suivant les étapes suivantes :

- $csl(Médecin_3, t'') = 4{,}021$.
- $Menace\_int(Médecin_3, l, F_p, c, t'') = 0{,}770$.
- $Menace(Médecin_3, l, F_p, c, t'') = 0{,}470$.
- $Impact\_int(Médecin_3, l, F_p, c, t'') = 5/6$.
- $Impact(Médecin_3, l, F_p, c, t'') = 5/6$.
- $Risque(Médecin_3, l, F_p, c, t'') = 0{,}391$.

D'après ce qui précède, l'accès de $Médecin_3$ au fichier F_p à l'instant *t''* représente l'accès le moins risqué *(0,391 < 0,3925 < 0,416)*.

Question 4

Si un médecin serait autorisé à lire le contenu du fichier F_p à l'instant *t''*, serait-il autorisé à le modifier au même instant *t''* ? Supposons que la valeur du risque acceptable pour les accès en écriture est égale à *0,05*. Est-ce que $Médecin_2$ ayant un niveau de confidentialité égal à *4,011* à l'instant *t*, après avoir accédé en lecture à un fichier ayant un niveau de confidentialité *5,3* à l'instant *t'*, serait autorisé à accéder en écriture au fichier F_p, à l'instant *t''*, sachant que l'effet des mesures de la réduction de la potentialité de la menace à considérer pour la demande d'accès de $Médecin_2$, en écriture, à F_p est égale à *0,2 ?*

Le calcul de la valeur du risque de l'accès en écriture de $Médecin_2$ consiste à suivre les étapes suivantes :

- $csl(Médecin_2, t'') = 5,321.$
- $Menace\_int(Médecin_2, e, F_p, c, t'') = 0,314.$
- $Menace(Médecin_2, e, F_p, c, t'') = 0,114.$
- $Impact\_int(Médecin_2, e, F_p, c, t'') = 5,321/6.$
- $Impact(Médecin_2, e, F_p, c, t'') = 5,321/6.$
- $Risque(Médecin_2, e, F_p, c, t'') = 0,101.$

D'après ce qui précède, $Médecin_2$ autorisé à lire le contenu du fichier F_p (son niveau de confidentialité ($5,321$) est supérieur au niveau de confidentialité de F_p (5)), ne serait pas autorisé à écrire dans le fichier F_p puisque la valeur du risque de cet accès est supérieure à la valeur du risque acceptable ($0,101 > 0,05$).

9.7.3 Cas 2

Considérons deux nouveaux intervenants : $Infirmière_1$ et $Infirmière_2$. Les niveaux de confidentialité et d'intégrité initiaux de ces deux infirmières sont comme suit :

1. $Infirmière_1$ a un niveau de confidentialité 4 et un niveau d'intégrité 3,
2. $Infirmière_2$ a un niveau de confidentialité 3 et un niveau d'intégrité 3.

Supposons aussi que $Inf(\{F_{p1}, F_{p2}\}) = 5$. En effet, la combinaison de l'information contenue dans les deux fichiers F_{p1} et F_{p2} permettrait de connaître des informations ayant un niveau de confidentialité supérieur au niveau de confidentilaité des informations de F_{p1} et F_{p2}.

L'historique d'accès des infirmières est comme suit :

1. $Infirmière_1$ a accédé en lecture au fichier F_{p1} ayant le niveau de confidentialité $4,08$ et le niveau d'intégrité 2,
2. $Infirmière_2$ a accédé en lecture à un fichier F_{p3} ayant le niveau de confidentialité 2 et le niveau d'intégrité 4.

Les deux infirmières demandent d'accéder en lecture au fichier F_{p2} ayant un niveau de confidentialité 4 à un instant t qui suit les accès cités dans les points 1 et 2.

9.7.3.1 Calcul du risque

A. Risque sur la confidentialité

Pour calculer le risque des accès des infirmières sur la confidentialité, nous utilisons les valeurs obtenues dans les étapes qui suivent.

Les niveaux de confidentialité des infirmières à l'instant *t* en considérant leur historique d'accès deviennent comme suit :

- $csl(infirmière_1, t) = 4,09.$
- $csl(infirmière_2, t) = 3.$

Les valeurs de potentialités intrinsèques de menaces des accès des infirmières à l'instant *t* en considérant leur historique d'accès sont comme suit :

- $Menace\_int(Infirmière_1, l, F_{p2}, c, t) = 0,768.$
- $Menace\_int(Infirmière_2, l, F_{p2}, c, t) = 0,657.$

Les valeurs d'impact intrinsèque des accès des infirmières à l'instant t en considérant leur historique d'accès sont comme suit :

- $Impact\_int(Infirmière_1, l, F_{p2}, c, t) = 5/6.$
- $Impact\_int(Infirmière_2, l, F_{p2}, c, t) = 4/6.$

Étant donné que la journalisation des accès n'est pas activée, l'effet de la mesure de sécurité m_1 n'est pas considérée, les valeurs de l'effet des mesures de sécurité réductrices de la potentialité des accès des infirmières sont comme suit :

- $Eff\_pot(Infirmière_1, l, F_{p2}, c, t) = 0,25.$
- $Eff\_pot(Infirmière_2, l, F_{p2}, c, t) = 0,25.$

Les valeurs de la potentialité de la menace des accès des infirmières sont calculées comme suit :

- $Menace(Infirmière_1, l, F_{p2}, c, t) = Menace\_int(Infirmière_1, l, F_{p2}, c, t) - Eff\_pot(Infirmière_1, l, F_{p2}, c, t) = 0,768 – 0,25 = 0,518.$
- $Menace(Infirmière_2, F_{p2}, l, c, t) = Menace\_int(Infirmière_2, l, F_{p2}, c, t) - Eff\_pot(Infirmière_2, l, F_{p2}, c, t) = 0,657 – 0,25 = 0,407.$

Les valeurs de l'effet des mesures de réduction de l'impact sont comme suit :

- *Eff_imp(Infirmière$_{1,}$ l, F_{p2}, c, t) = 0.*
- *Eff_imp(Infirmière$_{2,}$ l, F_{p2}, c, t) = 0.*

Les valeurs de l'impact des accès des infirmières sont calculées comme suit :

- *Impact(Infirmière$_1$, l, F_{p2}, c, t) = Impact_int(Infirmière$_1$, F_{p2}, l, c, t) - Eff_imp(Infirmière$_{1,}$ l, F_{p2}, c, t) = 5/6.*
- *Impact(Infirmière$_2$, l, F_{p2}, c, t) = Impact_int(Infirmière$_2$, l, F_{p2}, c, t) - Eff_imp(Infirmière$_{2,}$ l, F_{p2}, c, t) = 5/6.*

Les valeurs du risque des accès des infirmières sont calculées comme suit :

- *Risque(Infirmière$_1$, l, F_{p2}, c, t) = Menace(Infirmière$_1$, l, F_{p2}, c, t) × Impact(Infirmière$_1$, l, F_{p2}, c, t) = 0,518 × (5/6) = 0,431.*
- *Risque(Infirmière$_2$, l, F_{p2}, c, t) = Menace(Infirmière$_2$, l, F_{p2}, c, t) × Impact(Infirmière$_2$, l, F_{p2}, c, t) =0,407 × (5/6) = 0,339.*

D'après ce qui précède, Infirmière$_2$ sera autorisée à lire le fichier F_{p2} puisque son accès au fichier F_{p2} est le moins risqué (*0,339 < 0,431*).

B. Risque sur l'intégrité

Supposons que le niveau d'intégrité du fichier F_{p2} à l'instant *t* est *1*.

Les niveaux d'intégrité initiaux des infirmières sont comme suit :

- *isl(Infirmière$_1$, t_0) = 3.*
- *isl(Infirmière$_2$, t_0) = 3.*

Les niveaux d'intégrité des infirmières à l'instant *t* (*Voir la Formule 5 à la section 6.7.1 du chapitre 6*) deviennent comme suit :

- *isl(Infirmière$_1$, t) = 1,99999.*
- *isl(Infirmière$_2$, t) = 3.*

Les valeurs de la potentialité de la menace intrinsèque (*Voir la Formule 9 à la section 7.4.2.1 du chapitre 7*) des différents accès à l'instant *t* sont calculées comme suit :

- *Menace_int(Infirmière$_1$, l, F_{p2}, i, t) = 0,742.*
- *Menace_int(Infirmière$_2$, l, F_{p2}, i, t) = 0,771.*

Les valeurs de l'impact intrinsèque (*Voir la section 8.4 du chapitre 8*) des différents accès à l'instant *t* sont calculées comme suit :

- $Impact\_int(Infirmière_1, l, F_{p2}, i, t) = 4/5.$
- $Impact\_int(Infirmière_2, l, F_{p2}, i, t) = 4/5.$

Nous supposons que les valeurs des effets des mesures réductrices de la potentialité dans le cas des accès des infirmières lorsque l'intégrité est visée sont comme suit :

- $Eff\_pot(Infirmière_1, l, F_{p2}, i, t) = 0,2.$
- $Eff\_pot(Infirmière_2, l, F_{p2}, i, t) = 0,2.$

Les valeurs de la potentialité de la menace (*Voir la section 7.4.1.2 du chapitre 7)* des accès des infirmières à l'instant *t* lorsque l'intégrité est visée, sont calculées comme suit :

- $Menace(Infirmière_1, l, F_{p2}, i, t) = Menace\_int(Infirmière_1, l, F_{p2}, i, t) - Eff\_pot(Infirmière_1, l, F_{p2}, i, t) = 0,542.$
- $Menace(Infirmière_2, F_{p2}, l, i, t) = Menace\_int(Infirmière_2, l, F_{p2}, i, t) - Eff\_pot(Infirmière_2, l, F_{p2}, i, t) = 0,571.$

Les valeurs des effets des mesures réductrices de l'impact dans le cas des accès des infirmières lorsque l'intégrité est visée sont comme suit :

- $Eff\_imp(Infirmière_1, l, F_{p2}, i, t) = 0,3.$
- $Eff\_imp(Infirmière_2, l, F_{p2}, i, t) = 0,3.$

Les valeurs de l'impact des accès des infirmières à l'instant *t* lorsque l'intégrité est visée (*Voir la section 8.4 du chapitre 8*) sont calculées comme suit :

- $Impact(Infirmière_1, l, F_{p2}, i, t) = Impact\_int(Infirmière_1, l, F_{p2}, i, t) - Eff\_imp(Infirmière_1, l, F_{p2}, i, t) = 4/5 - 0,3 = 0,5.$
- $Impact(Infirmière_2, l, F_{p2}, i, t) = Impact\_int(Infirmière_2, l, F_{p2}, i, t) - Eff\_imp(Infirmière_2, l, F_{p2}, i, t) = 4/5 - 0,3 = 0,5.$

Les valeurs du risque des accès des infirmières à l'instant t lorsque l'intégrité est visée sont calculées comme suit :

- $Risque(Infirmière_1, l, F_{p2}, i, t) = Menace(Infirmière_1, l, F_{p2}, i, t) \times Impact(Infirmière_1, l, F_{p2}, i, t) = 0,271.$

- *Risque(Infirmière$_2$, l, F_{p2}, i, t) = Menace(Infirmière$_2$, l, F_{p2}, i, t) × Impact(Infirmière$_2$, l, F_{p2}, i, t) = 0,285.*

D'après ce qui précède, *Infirmière$_1$* pourrait être autorisée à lire le fichier F_{p2} puisque son accès au fichier F_{p2} est le moins risqué (*0,271 < 0,285*).

9.7.3.2 Considération simultanée de l'intégrité et de la confidentialité

Lorsque la valeur du risque acceptable pour l'intégrité est *0,275* et la valeur du risque acceptable pour la confidentialité est *0,450, Infirmière$_1$* serait autorisée à accéder au fichier F_{p2} puisque c'est la seule infirmière dont la valeur du risque d'accès au fichier F_{p2} lorsque l'intégrité est visée est inférieure à *0,275* et en même temps la valeur du risque du même accès, lorsque la confidentialité est visée, est inférieure à *0,450*.

9.8 Récapitulation

Dans le cas des accès en lecture lorsque la confidentialité est visée :

- le *risque* augmente lorsque la potentialité de la menace augmente.
- la potentialité de la menace augmente lorsque la potentialité de la menace intrinsèque augmente.
- la potentialité de la menace intrinsèque augmente lorsque les niveaux de confidentialité des sujets demandeurs d'accès, diminuent.
- les niveaux de confidentialité des sujets diminuent lorsque :
    - leurs niveaux de confidentialité initiaux diminuent.
    - les niveaux de confidentialité des entités à partir desquelles, ils ont reçu des flux d'informations, diminuent.
    - le nombre des flux d'information qu'ils ont reçu, diminue.
- la potentialité de la menace intrinsèque augmente lorsque les niveaux de confidentialité des objets augmentent.
- les niveaux de confidentialité des objets augmentent lorsque :
    - leurs niveaux de confidentialité initiaux augmentent.
    - les niveaux de confidentialité des entités à partir desquelles, ils ont reçu des flux d'informations, augmentent.
    - le nombre de flux d'informations qu'ils ont reçu, augmente.

- la potentialité de la menace augmente lorsque l'effet des mesures de sécurité réduisant la potentialité de la menace, diminue.
- le risque augmente lorsque l'impact augmente.
- l'impact augmente lorsque :
    - les niveaux de confidentialité des objets augmentent.
    - l'effet des mesures de sécurité réduisant l'impact diminue.

Dans le cas des accès en lecture lorsque la confidentialité est visée, le risque de l'accès d'un sujet à un objet augmente lorsque :

- le niveau de confidentialité initial du sujet diminue.
- le nombre des flux d'information, reçus par le sujet, diminue.
- les niveaux de confidentialité des entités ayant des flux d'information transmis au sujet, diminue.
- le niveau de confidentialité initial de l'objet auquel l'accès est demandé, augmente.
- les niveaux de confidentialité des entités ayant des flux d'informations transmis à l'objet auquel l'accès est demandé, augmentent.
- le nombre des flux d'information reçus par l'objet, augmente.
- l'effet des mesures de sécurité réduisant la potentialité de la menace diminue.
- l'effet des mesures de sécurité réduisant l'impact diminue.

Dans le cas des accès en écriture lorsque la confidentialité est visée, le risque de l'accès d'un sujet à un objet augmente lorsque :

- le niveau de confidentialité initial du sujet augmente.
- le nombre des flux d'information, reçus par le sujet, augmente.
- les niveaux de confidentialité des entités ayant transmis des flux d'informations au sujet demandeur d'accès, augmentent.
- le niveau de confidentialité initial de l'objet auquel l'accès est demandé, diminue.
- les niveaux de confidentialité des objets ayant des flux d'informations transmis à l'objet auquel l'accès est demandé, diminuent.
- le nombre des flux d'information reçus par l'objet, diminue.
- l'effet des mesures de sécurité réduisant la potentialité de la menace diminue.
- l'effet des mesures de sécurité réduisant l'impact diminue.

Dans le cas des accès en lecture lorsque l'intégrité est visée, le risque de l'accès d'un sujet à un objet augmente lorsque :

- le niveau d'intégrité initial du sujet augmente.
- le nombre des flux d'information, reçus par le sujet, augmente.
- les niveaux d'intégrité des entités ayant transmis des flux d'informations au sujet, augmentent.
- le niveau d'intégrité initial de l'objet auquel l'accès est demandé, diminue.
- les niveaux d'intégrité des entités ayant des flux d'informations transmis à l'objet, diminuent.
- le nombre des flux d'information reçus par l'objet, diminue.
- l'effet des mesures de sécurité réduisant la potentialité de la menace diminue.
- l'effet des mesures de sécurité réduisant l'impact diminue.

Dans le cas des accès en écriture lorsque l'intégrité est visée, le risque de l'accès d'un sujet à un objet augmente lorsque :

- le niveau d'intégrité initial du sujet diminue.
- le nombre des flux d'information, reçus par le sujet, diminue.
- les niveaux d'intégrité des entités ayant transmis des flux d'informations au sujet, diminuent.
- le niveau d'intégrité initial de l'objet auquel l'accès est demandé, augmente.
- les niveaux d'intégrité des entités ayant des flux d'informations transmis à l'objet auquel l'accès est demandé, augmentent.
- le nombre des flux d'informations reçus par l'objet, augmente.
- l'effet des mesures de sécurité réduisant la potentialité de la menace diminue.
- l'effet des mesures de sécurité réduisant l'impact diminue.

9.9 Conclusion

L'approche de calcul du risque des requêtes d'accès que nous avons présentée dans cette thèse traite les cas où un sujet utilise ses accès légitimes pour effectuer une action qui viole la politique de contrôle d'accès. L'utilisation de cette approche a été démontrée dans deux cas d'application.

Une caractéristique intéressante de notre approche réside dans son aspect dynamique, en effet un accès accepté à un instant donné peut être refusé si le même accès est demandé à un instant ultérieur. De même, un accès refusé à un instant donné peut être accepté s'il est demandé à un instant ultérieur. Cela peut être le résultat du changement du niveau de sécurité du sujet et/ou du niveau de sécurité de l'objet, du changement de l'effet des mesures de sécurité mises en place ou du changement du niveau de risque maximal acceptable. De plus, les réponses aux demandes d'accès pourraient être différentes selon l'action demandée (lecture ou écriture).

Notre approche permet de spécifier des politiques que nous ne pouvons pas spécifier avec les modèles traditionnels et permet de choisir les sujets et les objets dont l'intégration dans les tâches des flux de travail, représente moins de risque sur la confidentialité et/ou l'intégrité. De plus, notre approche est applicable au modèle *ABAC (Voir la section 9.2 de ce chapitre).*

L'approche présentée dans ce travail serait utile dans les environnements collaboratifs [6, 66] et ubiquitaires [95] où de nombreux utilisateurs distants géographiquement travaillent ensemble pour accomplir certaines tâches et où des contraintes sur les flux d'informations peuvent exister. De surcroît, elle permet une administration décentralisée puisque les politiques de contrôle d'accès peuvent être mises à jour automatiquement en fonction de l'historique des accès, des mesures de sécurité et du niveau du risque acceptable.

Chapitre 10 : Implémentation

10.1 Introduction

Dans ce chapitre, nous présentons l'outil *IFARBAC* (*Information Flow And Risk Based Access Control*) que nous avons développé pour simuler notre approche. Cet outil permet de calculer et afficher les niveaux de sécurité et le risque des requêtes d'accès. Il permet aussi d'afficher les décisions d'accès et les journaliser.

En utilisant cet outil, un utilisateur peut se connecter, demander l'accès aux objets et consulter son niveau de sécurité courant. De plus, un administrateur peut ajouter des sujets et des objets, leur attribuer des niveaux de sécurité initiaux, entrer le niveau de risque acceptable et le nombre de niveaux de sécurité des sujets et des objets.

10.2 Langages et plateforme

Pour développer l'outil *IFARBAC*, nous avons eu recours à *EasyPHP* [42] qui est une plateforme de développement *Web*, permettant de faire fonctionner localement des scripts *PHP*. *EasyPHP*est un environnement qui comprend un serveur web *Apache* et un serveur de bases de données *MySQL*, un interpréteur de script (*PHP*) [88] qui est un langage de programmation libre utilisé pour produire des pages *Web* dynamiques, ainsi qu'une administration *SQL phpMyAdmin*.

10.3 Démonstration de notre approche

La *Figure 49* représente l'interface de connexion.

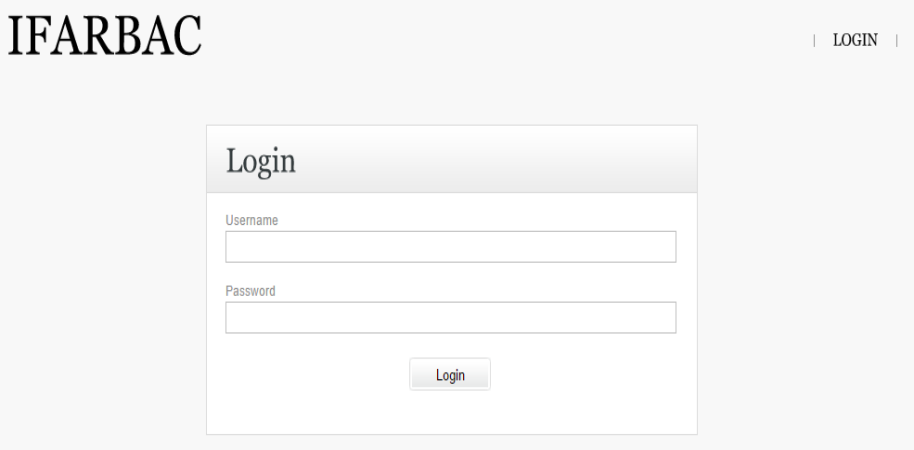


Figure 49. Interface de connexion

La *Figure 50* montre l'interface qui s'affiche suite à l'authentification d'un utilisateur. Cette interface affiche l'objectif de sécurité visé, le niveau *courant* du sujet connecté, les objets, les niveaux de sécurité des objets et les droits d'accès à demander. Une requête d'accès s'exécute en cliquant sur l'action demandée.

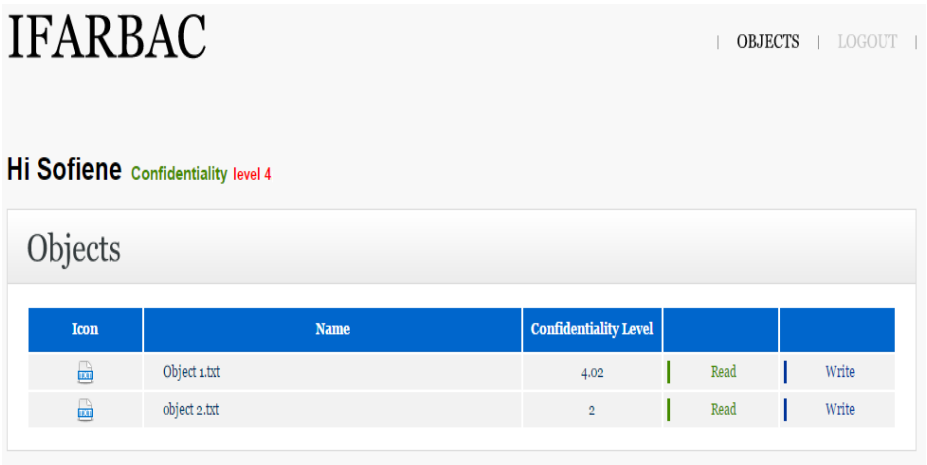


Figure 50. Interface pour la demande d'accès

La *Figure 51* représente l'interface qui permet à l'administrateur d'afficher les objets existants et d'ajouter des objets.

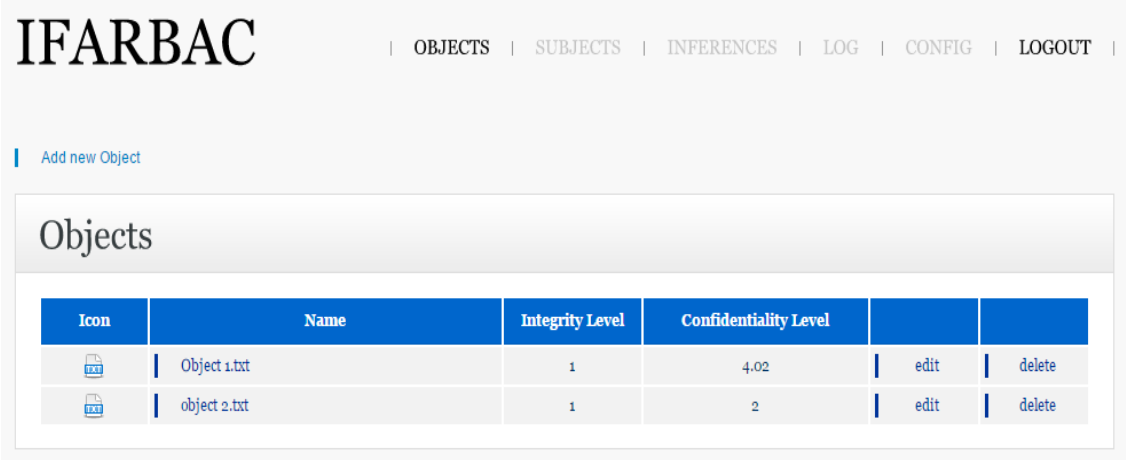


Figure 51. Interface d'affichage des objets

La *Figure 52* représente l'interface qui permet à l'administrateur d'ajouter des sujets et leurs niveaux de sécurité. Une interface semblable a été développée pour permettre à l'administrateur d'ajouter les objets et leurs niveaux de sécurité.

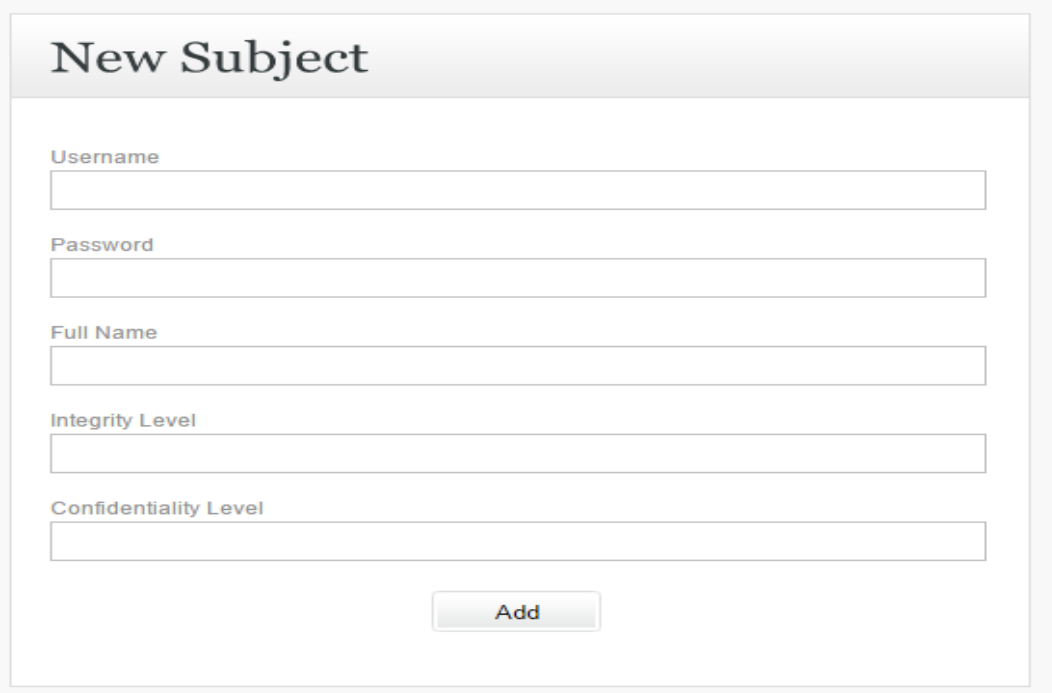


Figure 52. Interface d'ajout des sujets

La *Figure 53* représente l'interface qui permet à l'administrateur d'entrer la valeur du risque acceptable, le nombre des niveaux de sécurité. Elle lui permet également de choisir l'objectif de sécurité à considérer.

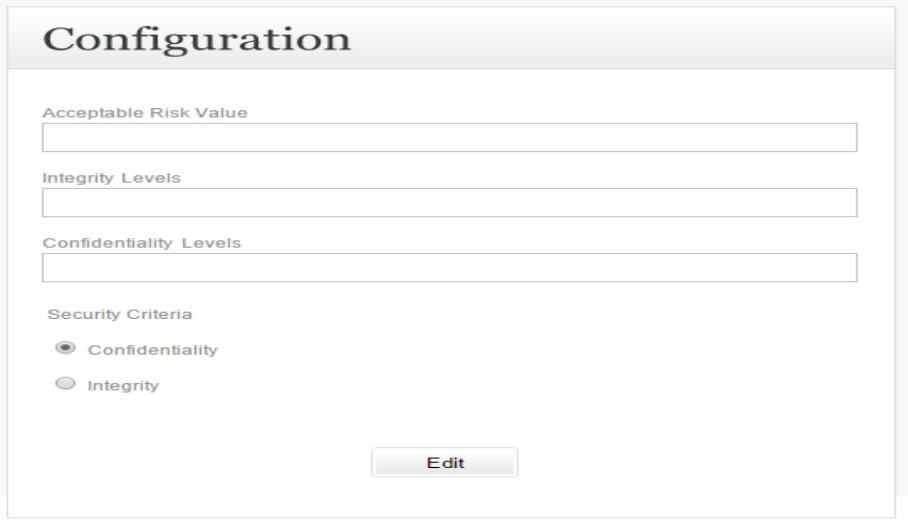


Figure 53. Interface de configuration

La *Figure 54* représente l'interface qui permet à l'administrateur d'entrer les objets dont la combinaison permet de déduire de nouvelles informations à considérer pour le calcul des niveaux de sécurité et le calcul du risque des requêtes d'accès. L'interface permet aussi de donner un nom à une inférence, de sélectionner les objets impliqués et le niveau de sécurité de l'information à obtenir de cette inférence.

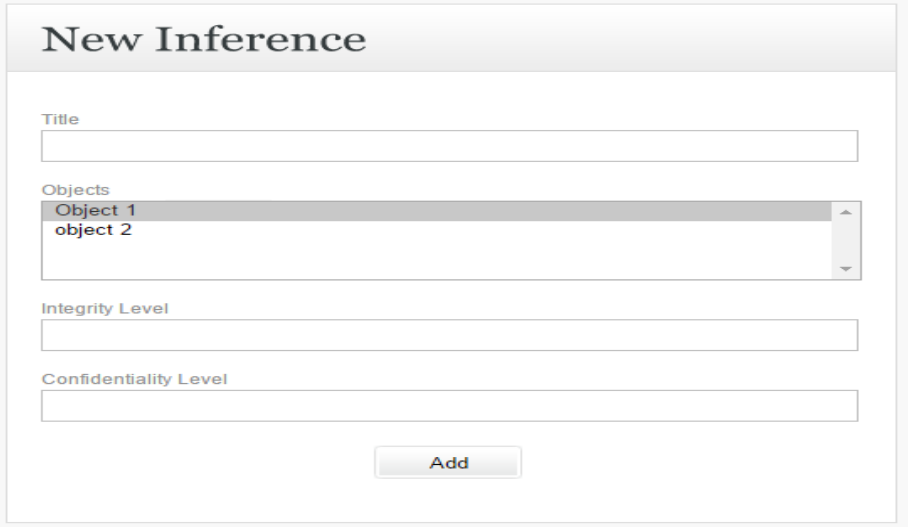


Figure 54. Interface de définition des inférences

Les trois figures suivantes représentent les interfaces qui s'affichent suite à une demande d'accès :

La *Figure 55* représente l'interface qui s'affiche suite è une demande d'accès acceptable par défaut.

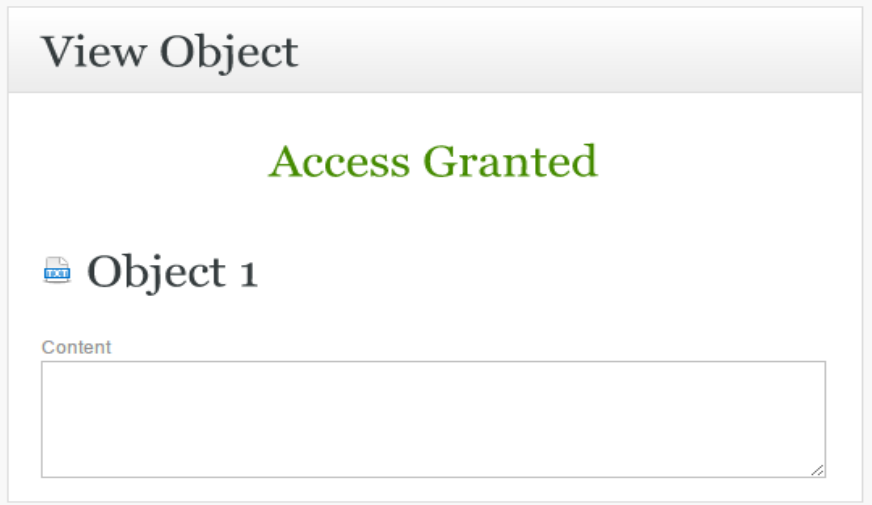


Figure 55. Demande d'accès acceptée par défaut

La *Figure 56* représente l'interface qui s'affiche lorsqu'une demande d'accès est acceptée suite au calcul du risque. L'interface montre que l'accès a été accepté car la valeur du risque associée à la requête d'accès *(0,269)* est inférieure à la valeur du risque acceptable *(0,6)*.

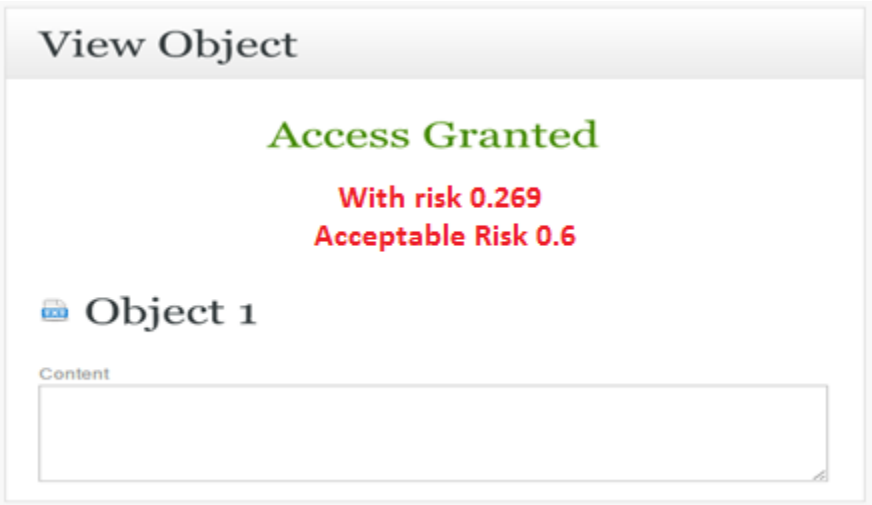


Figure 56. Demande d'accès acceptée suite à un calcul du risque

La *Figure 57* représente l'interface qui s'affiche lorsqu'une demande d'accès est refusée suite au calcul du risque. L'interface montre que l'accès a été refusé car la valeur du risque associée à la requête d'accès (*0,269*) est supérieure à la valeur du risque acceptable (*0,1*).

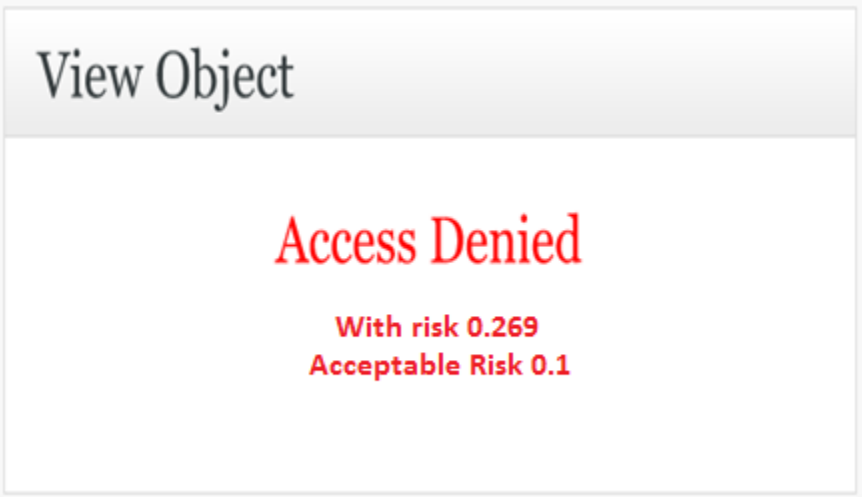


Figure 57. Demande d'accès refusée suite au calcul du risque

La *Figure 58* représente l'interface qui affiche la journalisation des accès passés.

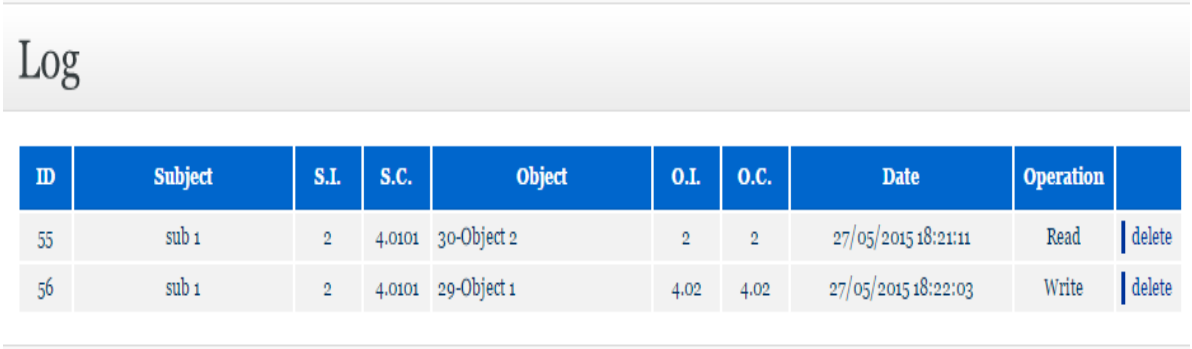


Figure 58. Journaux d'accès

10.4 Temps d'exécution

Étant donné que notre méthode implique l'ajout de quelques calculs aux méthodes de contrôle d'accès déjà établies, on pourrait s'interroger si elle a des effets négatifs sur les temps d'exécution. Au contraire, notre approche n'a qu'une incidence minime sur le temps d'exécution. Nous proposons seulement de garder des traces de l'historique des accès et de faire quelques calculs, ce qui peut être fait en un temps négligeable. Notre approche n'ajoute aucune nouvelle opération de fichier ni de communications interprocessus. Pour

le calcul du risque, nous avons recours seulement à des opérations arithmétiques et des opérations de lecture des mesures de sécurité à partir d'une table, cela peut être fait également en un temps négligeable. En effet, le temps d'exécution de notre algorithme est la somme des temps d'exécution d'un ensemble d'algorithmes qui sont de complexité *constante O(1), linéaire O(n)* et *polynômiale* $O(n^i)$.

Évaluation du temps d'exécution de l'algorithme de calcul des niveaux de sécurité

Le temps d'exécution de l'algorithme de calcul des niveaux de sécurité est la somme du temps d'exécution de deux sous algorithmes : la complexité du premier est linéaire alors que la complexité du second est polynômiale.

Prenons le cas de la *Formule 1* de la section *6.7.1* :

$$csl(s, t) = Max(KnSL_cA(s, t))+(\sum_{i=1}^{|Lc|} Num(i, (KnSL_cA(s, t) - \{Max(KnSL_cA(s, t))\})))\times 10^{-k\,((|Lc|+1)- i)}$$

- $Max(KnSL_cA(s, t))$: le sous algorithme utilisé pour implémenter cette partie de la formule consiste à parcourir un tableau contenant les niveaux de sécurité pour trouver la valeur maximale. Le paramètre de complexité est la taille du tableau *(n)*. Il s'agit d'une augmentation **linéaire** *O(n)* du temps d'exécution quand la taille du tableau croit (si le paramètre de complexité double, le temps double). Notons que la complexité de l'algorithme utilisé pour ajouter les niveaux de sécurité dans le tableau est également linéaire (une seul boucle).

- $\sum_{i=1}^{|Lc|} Num(i, (KnSL_cA(s, t) - \{Max(KnSL_cA(s, t))\})) \times 10^{-k\,((|Lc|+1)- i)}$: le sous algorithme utilisé pour implémenter cette partie de la formule consiste à utiliser 2 boucles imbriquées. Lorsque le paramètre de complexité *n* double, le temps d'exécution est multiplié par n^i. Il s'agit d'une complexité **polynômiale** $O(n^i)$. Dans le cas de ce sous algrithme, *i* est égale à *2*, il s'agit plus précisément d'une complexité **quadratique**. En effet, lorsque le paramètre de complexité double, le temps d'exécution est multiplié par *4*.

Évaluation du temps d'exécution de l'algorithme de calcul de la potentialité de la menace, de l'impact et du risque

Les algorithmes utilisés pour implémenter les formules de calcul de la potentialité de la menace, de l'impact et du risque ont une complexité **consatnte** *O(1)*. Il n'y a pas d'augmentation du temps d'exécution quand le paramètre de complexité croit. En effet, il s'agit d'opérations d'addition, de multiplication, de soustratction et de divisions dans le cas du premier algorithme, d'opérations de division et de soustraction dans le cas du second et d'une simple opération de multiplication des valeurs obtenues par les deux premiers algorithmes dans le cas du troisième.

10.5 Conclusion

Dans ce chapitre, nous avons présenté l'outil que nous avons développé pour simuler notre approche de calcul du risque qui inclut le calcul des niveaux de sécurité des sujets et des objets. De surcroît, nous avons expliqué que les incidences de notre approche sur le temps d'exécution, sont négligeables.

Chapitre 11 : Conclusion

11.1 Travail accompli

Dans cette thèse, nous avons identifié et développé en détail une approche basée sur les *flux d'informations* pour *le calcul du risque* des requêtes d'accès. Cette approche permet d'éviter certaines limites du contrôle d'accès traditionnel basé sur des décisions d'accès statiques et rigides, et offre la possibilité de répondre aux besoins d'accès changeants des entreprises tout en prenant en considération la sécurité des informations.

11.1.1 Notre approche

L'approche que nous avons présentée dans cette thèse peut être vue comme une approche de calcul du risque de la violation d'une politique de contrôle d'accès suite à l'autorisation d'une requête d'accès. Elle traite les cas où un employé utilise ses accès légitimes pour effectuer une action qui viole la politique de contrôle d'accès : divulguer des données sensibles à une tierce partie, fournir des renseignements à un employé qui n'a pas le droit de les connaître, etc. Elle consiste essentiellement à considérer l'habilitation dynamique du sujet demandeur d'accès, la classification dynamique de l'objet à accéder ainsi que les mesures de sécurité mises en place pour déterminer la *potentialité de la menace* et l'*impact* d'une requête d'accès. Cette approche, représentée par la *Figur*e *59*, consiste à suivre les grandes étapes suivantes :

1. calculer les *niveaux de sécurité* du sujets et de l'objet en considérant les flux d'informations générés par les accès qui ont été autorisés,
2. calculer la *potentialité intrinsèque de la menace* et l'*impact intrinsèque* de la requête d'accès,
3. calculer la *potentialité de la menace* et l'*impact* de la requête d'accès en tenant compte des mesures de sécurité de réduction de la potentialité de la menace et de l'impact,
4. calculer le *risque* de la requête d'accès.

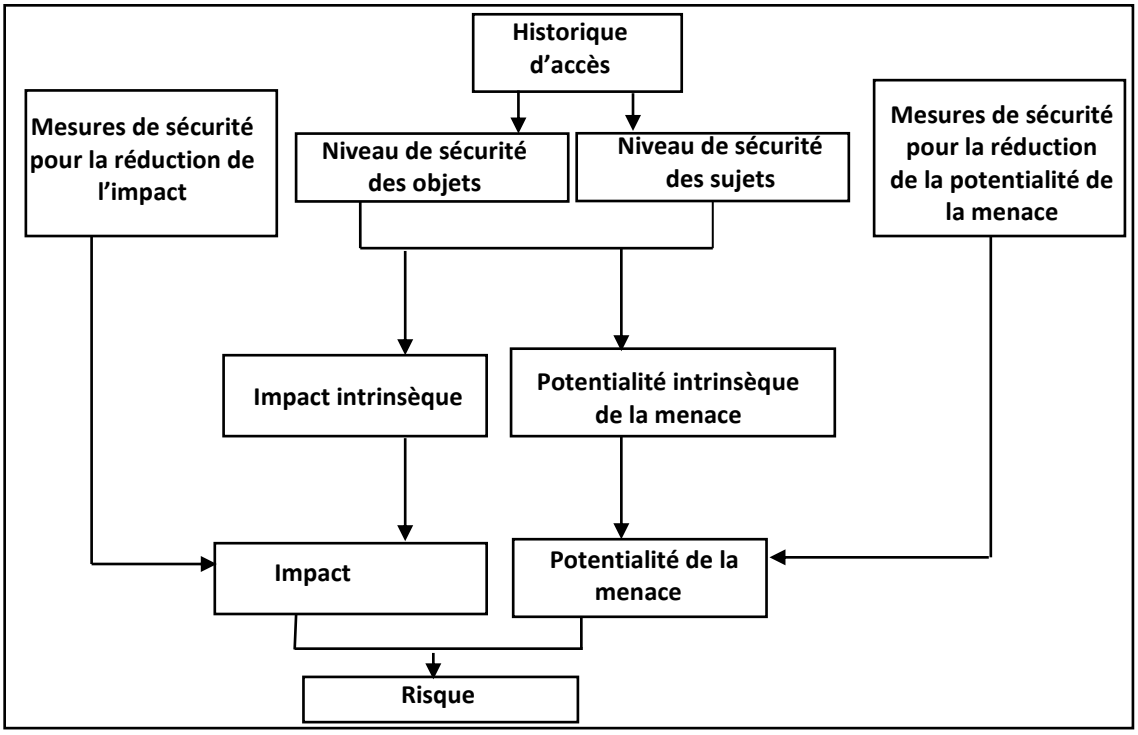


Figure 59. Approche de calcul du risque des requêtes d'accès

Dans cette thèse, nous avons adopté des concepts de *gestion du risque* et plus précisément de la méthodologie *Méhari* [23], pour intégrer l'effet des mesures de sécurité mises en place à notre approche. Ces mesures de sécurité sont des moyens de gérer le risque et peuvent être de nature administrative, technique, ou juridique. Nous avons distingué deux familles de mesures de sécurité :

- Les mesures de sécurité qui permettent de réduire la valeur de la potentialité de la menace (p. ex. la journalisation des accès).
- Les mesures de sécurité qui permettent de réduire la valeur de l'*impact* (p. ex. les copies de sauvegarde).

La considération de l'effet des mesures de sécurité réductrices de la potentialité de la menace et de l'impact permet de changer les valeurs du risque. Cela permet d'obtenir des évaluations plus réalistes.

Les étapes de cette approche sont brièvement rappelées dans ce qui suit.

11.1.1.1 Calcul des niveaux de sécurité

Notre approche de calcul des niveaux de sécurité est une approche dynamique basée sur l'historique des accès pour tenir compte des flux d'informations. Elle a été développée via des exemples, des principes, des définitions formelles et des formules afin d'évaluer les niveaux de confidentialité et d'intégrité des sujets et des objets. Cette approche tient compte des inférences d'informations (association et agrégation d'informations) lorsque la confidentialité est visée.

Notre approche est basée essentiellement sur les principes qui stipulent que les niveaux de confidentialité des entités augmentent lorsqu'elles reçoivent des flux d'informations et que leurs niveaux d'intégrité diminuent lorsqu'elles reçoivent des flux d'informations à partir d'autres entités ayant des niveaux d'intégrité plus bas.

L'application de cette approche est la première étape de notre méthode de calcul du risque des requêtes d'accès, qui se base principalement sur les niveaux de sécurité. Cependant, cette approche peut être utilisée séparément de l'approche globale d'analyse de risque présentée dans cette thèse.

Notons qu'une partie du travail présenté dans le chapitre *6* de cette thèse a fait l'objet de notre article [12].

11.1.1.2 Calcul de la potentialité de la menace

L'évaluation de la potentialité de la menace est un prérequis pour évaluer les risques d'accès. Le calcul de la potentialité de la menace passe par le calcul de la potentialité intrinsèque de la menace qui est une évaluation maximaliste de la possibilité de l'occurrence du risque, sans la considération des mesures de sécurité [23].

Pour calculer les potentialités de menaces des accès, nous avons considéré des modèles des menaces internes (*modèle CMO*) [86, 99-101] et nous avons défini des principes qui considèrent essentiellement les niveaux de sécurité des sujets et des objets, et par conséquent les flux d'informations résultants de ces accès. Cette approche est basée sur l'hypothèse qui considère que la *potentialité intrinsèque de la menace* dépend de l'importance des flux d'informations entre les niveaux de sécurité des objets et les niveaux de sécurité des sujets. Autrement dit, nous avons supposé une *corrélation* entre les flux d'information qui peuvent résulter d'un accès et la *potentialité intrinsèque de la menace*.

Notre approche pour le calcul de la *potentialité de la menace* considère les facteurs suivants :

- L'*objectif de sécurité* visé (confidentialité ou intégrité).
- L'*action demandée* (lecture ou écriture).
- La *motivation* qui peut être déduite à partir des *caractéristiques personnelles* des utilisateurs permettant d'évaluer à quel point un groupe d'employés est fiable ou à quel point il peut être motivé à concrétiser la menace. Dans notre approche, ce facteur est représenté par le *niveau de confidentialité* ou le *niveau d'intégrité* du sujet demandeur d'accès.
- L'*opportunité* qui représente la tentation causée par l'attribution du nouveau privilège. Dans notre approche, ce facteur est représenté par le *niveau de confidentialité* ou le *niveau d'intégrité* de l'objet à accéder.
- Les *mesures de sécurité réductrices de la potentialité de la menace* (mesures structurelles, mesures dissuasives et mesures préventives).

Certaines idées partiellement similaires aux nôtres concernant le calcul de la potentialité de la menace, ont fait l'objet de nos articles [60, 61]. Cependant, les idées présentées dans cette thèse, en lien avec le calcul de la potentialité de la meance, ont fait l'objet de nos articles [13, 14].

11.1.1.3 Calcul de l'impact

De façon générale, l'impact représente la gravité des conséquences directes et indirectes qui découleraient de l'occurrence du risque (divulgation ou altération des informations). La gravité des conséquences de l'occurrence du risque dépend de l'importance de la confidentialité ou de l'intégrité des informations contenues dans les objets et connues par le sujet.

Le calcul de l'impact passe par le calcul de l'*impact intrinsèque* qui est une évaluation maximaliste de la possibilité de l'occurrence du risque, sans la considération des mesures de sécurité [23].

Pour calculer l*'impact*, nous avons considéré que la valeur de l'*impact* est proportionnelle à la valeur du niveau de confidentialité de l'entité (sujet ou objet) *source de l'information* de laquelle, nous soustrayons la valeur de l'efficacité des mesures de

sécurité pour la réduction de l'impact, lorsque la confidentialité est visée. De même, nous avons considéré que la valeur de l'*impact* est inversement proportionnelle à la valeur du niveau d'intégrité de l'entité (sujet ou objet) *source de l'information*, de laquelle nous soustrayons la valeur d'efficacité des mesures de sécurité pour la réduction de l'impact, lorsque l'intégrité est visée. Ainsi, notre approche nous a permis d'obtenir des valeurs d'impact évolutives.

11.1.1.4 Calcul du risque

Pour rendre plus flexibles des modèles de contrôle d'accès connus, nous avons adapté la formule de calcul du risque de l'*OWASP* comme suit :

$$Risque(s, a, o, ob, t) = Menace(s, a, o, b, t) \times Impact(s, a, o, ob, t)$$

11.2 Contributions

La contribution originale de notre thèse est une approche dynamique raffinée pour le calcul du risque pour les systèmes de contrôle d'accès qui permet d'améliorer les décisions d'accès à prendre. Pour calculer la valeur finale du risque, nous avons défini un ensemble de formules basées sur la connaissance des flux d'informations. De plus, nous avons montré que notre approche est applicable pour les systémes de contrôle d'accès *ABAC*.

11.2.1 Approche de calcul du risque

Notre approche est caractérisée par son aspect dynamique, un accès accepté à un instant donné peut être refusé s'il est demandé à un instant ultérieur et un accès refusé à un instant donné peut être accepté s'il est demandé à un instant ultérieur. Cela peut être le résultat du changement du niveau de sécurité du sujet et/ou du niveau de sécurité de l'objet, du changement de l'effet des mesures de sécurité mises en place ou du changement du niveau de risque maximal acceptable. De plus, les réponses aux demandes d'accès pourraient être différentes selon l'action demandée (lecture ou écriture).

Notre approche permet de spécifier des politiques de contrôle d'accès qu'il n'est pas possible de spécifier avec les modèles de contrôle d'accès traditionnels, et permet de choisir les sujets et les objets qui représentent moins de risque pour les inclure dans les tâches des flux de travail. Cela n'est pas possible avec d'autres approches de contrôle d'accès.

De surcroît, nous avons défini des propriétés pour déterminer un *ordre de priorité* sur les *niveaux de sécurité* des sujets et des objets. De même, nous avons défini des propriétés pour déterminer un *ordre de priorité* sur les *potentialités des menaces* et les *impacts* des accès.

Notons que notre approche peut être appliquée dans le cas des systèmes de contrôle d'accès où certaines décisions sont souvent basées sur le calcul du risque comme elle peut être appliquée pour déroger aux politiques de contrôle d'accès prédéfinies seulement dans certaines situations particulières.

11.2.2 Formules développées

Pour rendre possible une implémentation précise de notre approche, nous avons développé dans les chapitres *5*, *6*, *7* et *8*, des formules qui permettent de calculer les risques des demandes d'accès. Dans le chapitre *5*, nous avons présenté une formule de calcul du risque. Dans le chapitre *6*, nous avons présenté des formules pour le calcul des niveaux de confidentialité et d'intégrité des sujets et des objets. Dans le chapitre *7*, nous avons pésenté des formules pour le calcul de la potentialité de la menace sur la confidentialité et sur l'intégrité dans le cas des accès en lecture et d'écriture. Dans le chapitre *8*, nous avons présenté des formules pour le calcul de l'impact sur la confidentialité et sur l'intégrité dans le cas des accès en lecture et en écriture. Cependant, nous soulignons que les idées de notre méthode sont indépendantes des formules et donc pourraient être implémentées avec des formules différentes.

11.2.3 Application au modèle ABAC

Pour l'implémentation de notre méthode de calcul du risque dans le modèle *ABAC*, nous avons ajouté un calculateur des niveaux de sécurité, un calculateur du risque ainsi qu'un *point de politique du risque PRP*. Selon notre approche, l'historique des accès sera transmis au calculateur des niveaux de sécurité, aussi les niveaux de sécurité mis à jour et les évaluations des mesures de sécurité mises en place, seront transmis au calculateur du risque. Les mesures de sécurité sont considérées comme des facteurs de l'environnement à

en tenir compte pour calculer le risque avant de déterminer les décisions d'accès *(Voir la section 9.2 du chapitre 9)*.

11.2.4 Implémentation

Nous avons implémenté notre outil *IFRABAC* (*Information Flow and Risk Based Access Control*) présenté dans le chapitre *10*. Cet outil permet de calculer et d'afficher les niveaux de sécurité des sujets et des objets, et les valeurs du risque. Il permet également d'afficher les décisions d'accès et de les journaliser.

11.2.5 Cas d'application

Dans la section *9.6* du chapitre *9*, nous avons présenté un cas d'application qui décrit un scénario d'usage de notre approche et qui montre la possibilité de son application réelle, afin de faciliter le partage d'informations, tout en tenant compte des risques sur la sécurité de l'information.

11.2.6 Comparaison aux modèles de la littérature

Dans cette section, nous comparons notre méthode de calcul des niveaux de sécurité aux modèles MLS traditionnels. Par la suite, nous comparons notre méthode de calcul du risque à des méthodes de contrôle d'accès basées sur le risque.

11.2.6.1 Comparaison de notre méthode de calcul des niveaux de sécurité aux modèles MLS traditionnels

Le *Tableau 72* compare différents modèles de sécurité *MLS*, y compris le nôtre, en tenant compte d'un ensemble de critères.

Approche	*Niveaux de sécurité*	*Valeurs des niveaux de sécurité*	*Objectifs de sécurité*	*Historique d'accès*	*Décisions d'accès*
Bell-Lapadula	*Statiques*	*Entiers naturels* *Nombre limité*	*Confidentialité*	*Non considéré* *Non reflété*	*Statiques*
BIBA	*Statiques*	*Entiers naturels* *Nombre limité*	*Intégrité*	*Non considéré* *Non reflété*	*Statiques*
Plus haut niveau	*Dynamiques puis statiques*	*Entiers naturels* *Nombre limité*	*Confidentialité*	*Considéré partiellement* *Non reflété*	*Dynamiques puis statiques*
Plus bas niveau	*Dynamiques puis statiques*	*Entiers naturels* *Nombre limité*	*Intégrité*	*Considéré partiellement* *Non reflété*	*Dynamiques puis statiques*
Notre approche	*Dynamiques*	*Réels* *Grand nombre*	*Confidentialité* *Intégrité*	*Considéré* *Reflété*	*Dynamiques raffinées*

Tableau 71. Comparaison de notre méthode de calcul des niveaux de sécurité aux modèles MLS traditionnels

Ce tableau permet de voir que notre méthode de calcul des niveaux de sécurité est la seule approche parmi les méthodes d'accès présentées dans ce tableau, qui :

- fournit une estimation dynamique des niveaux de sécurité sous forme de réels offrant ainsi plus de précision (Les autres méthodes considérent généralement un nombre très limité de niveaux de sécurité exprimés par des entiers naturels),
- considère l'historique des accès (par conséquent les flux d'information), et le reflète,
- permet d'avoir des décisions d'accès dynamiques raffinées,
- s'applique lorsque les objectifs de confidentialité et d'intégrité sont visés.

11.2.6.2 Comparaison de notre méthode de calcul du risque à d'autres méthodes de contrôle d'accès basées sur le risque

Le *Tableau 73* compare différents travaux d'évaluation du risque pour les systèmes de contrôle d'accès, y compris le nôtre, en tenant compte d'un ensemble de critères.

Approche	***Estimation***	***Modèle traditionnel***	***Estimation des mesures de sécurité mises en place***	***Opérations***	***Objectif de sécurité***	***Historique d'accès***
RADAC	*Non applicable*	*Tous les modèles*	*Non*	*Tous les accès*	*Sans distinction*	*Non*
RADAC-UCON	*Non applicable*	*ABAC*	*Non*	*Tous les accès*	*Sans distinction*	*Non*
Dérogation-RBAC	*Qualitative*	*RBAC*	*Non*	*Tous les accès*	*Sans distinction*	*Non*
RBAC-risque	*Quantitative*	*RBAC*	*Non*	*Tous les accès*	*Sans distinction*	*Non*
Multiniveaux-floue	*Quantitative*	*MLS*	*Non*	*Lecture*	*Confidentialité*	*Non*
Risque dans les systèmes de santé	*Quantitative*	*Tous les modèles*	*Non*	*Tous les accès*	*Sans distinction*	*Oui*
Inférence floue	*Quantitative*	*MLS*	*Non*	*Lecture*	*Confidentialité*	*Oui*
Notre approche	*Quantitative Qualitative*	*MLS ABAC*	*Oui*	*Lecture Écriture*	*Confidentialité Intégrité*	*Oui*

Tableau 72. Comparaison de notre approche aux méthodes de contrôle d'accès basées sur le risque

Ce tableau permet de voir que notre approche est la seule approche parmi les méthodes d'accès présentées dans ce tableau qui, en même temps, :

- fournit une estimation quantitive et qualitative des risques des accès,
- s'applique aux modèles de sécurité multi-niveaux *MLS* et au modèle de contrôle d'accès basé sur les attributs *ABAC*,
- tient compte des mesures de sécurité réductrices du risque conformément à la littérature en gestion des risques,

- fournit des valeurs séparées pour les objectifs de sécurité de confidentialité et d'intégrité,
- considère l'historique des accès, permettant ainsi une évaluation dynamique du contenu des entités (sujets et objets) et par conséquent des décisions d'accès dynamiques raffinées.

11.3 Limites de notre approche

Il est important d'observer que notre approche ne permet pas de se protéger contre les attaques par *Cheval de Troie* puisque les règles obligatoires des modèles de sécurité multiniveaux traditionnels ne sont pas respectées [83]. En effet, le non-respect de ces règles pourrait générer des fuites d'informations en permettant le passage de ce type de programmes malveillants vers des entités ayant des niveaux de confidentialité élevés. Le problème de développer une approche capable de répondre à ces exigences ainsi qu'aux nôtres reste ouvert.

De plus, notre approche ne permet pas de calculer le risque sur la *disponibilité* et se limite à la *confidentialité* et à l'*intégrité*. Elle se limite aux opérations de lecture et d'écriture, et ne permet pas de calculer le risque d'autres opérations (suppression, exécution, création d'objets, etc.), ainsi que d'autres opérations non reliées aux données. En outre, elle ne permet pas l'estimation des risques d'*ingénierie sociale e*t de *déni de service*.

Une autre limite à mentionner, serait la nécessité de l'attribution de niveaux de sécurité initiaux à tous les sujets et les objets. Cette tâche pourrait être complexe et coûteuse dans le cas d'une grande organisation. Cela dit, la classification des objets doit être mise en œuvre dans les organisations, non pas seulement pour contrôler les accès, mais pour déterminer les mesures de sécurité appropriées à mettre en place [37, 38, 56].

Notre approche ne considère pas non plus les catégories des informations, qui permettent d'exprimer le *besoin de savoir* [83], un facteur important pour l'évaluation des risques des demandes d'accès.

L'application de notre approche pourrait impliquer l'augmentation des privilèges des sujets donnant ainsi lieu à des politiques d'accès trop permissives. Nous pensons que

l'application de notre approche doit passer par une définition claire des besoins de sécurité pour assurer son utilisation optimale. En effet, étant donné que notre approche représente un cadre général pour la précision des décisions d'accès, son utilisation partielle ou sa combinaison avec des méthodes de contrôle d'accès traditionnels pourrait donner une solution à ce problème. Exemple : utilisation des niveaux de sécurité évolutifs seulement dans le cas des demandes d'accès en écriture ou seulement pour certains sujets. Une solution générique à ce problème fera l'objet de nos travaux futurs.

11.4 Travaux futurs

Une orientation future de nos travaux, consiste à considérer explicitement d'autres facteurs pour la détermination du risque d'une requête d'accès tels que l'emplacement physique ou l'emplacement logique des sujets et des objets.

Nous comptons aussi considérer le besoin de savoir en tenant compte du concept des catégories d'informations.

Nous prévoyons également la considération des besoins opérationnels ainsi que l'utilisation des *obligations* qui seraient des activités devant être réalisées par des sujets ou sur les objets avant ou lors d'un accès, pour diminuer le risque.

De surcroît, nous explorerons l'application de notre approche dans le contexte des systèmes *RBAC*.

Nous continuerons également à améliorer certains aspects de notre approche pour pallier aux limites mentionnées dans la section précédente.

Bibliographie

[1] Agence nationale de la sécurité des systèmes d'informations.: Le déni de service distribué (2000)

[2] Agrawal, D.: A new schema for security in dynamic uncertain environments. Sarnoff Symposium. 1–5. (2009)

[3] Ahn, G., Shin, M.: Role-based authorization constraints specification using object constraint language. 10th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises. 157–162 (2001)

[4] Audit Commission: Opportunity Makes a Thief: An Analysis of Computer Abuse. HM Stationery Office. (1994)

[5] Balepin, I., Maltsev, S., Rowe, J., Levitt, K.: Using specification-based intrusion detection for automated response. Recent Advances in Intrusion Detection. 136– 154. (2003).

[6] Banks, D., Erickson, J. S. Rhodes, M.: Toward cloud-based collaboration services. Usenix Workshop on Hot Topics in Cloud Computing. (2009)

[7] Bartsch, S.: A calculus for the qualitative risk assessment of policy override authorization. 3rd international conference on Security of information and networks. 62–70 (2010)

[8] Bell, D. E., La Padula, L. J.: Secure computer system: Unified exposition and multics interpretation. DTIC Document, Technical report. (1976)

[9] Biba, K. J.: Integrity considerations for secure computer systems. DTIC Document, Technical report. (1977)

[10] Bishop, M., Gates, C.: Defining the insider threat. 4th annual workshop on Cyber security and information intelligence research: Developing strategies to meet the cyber security and information intelligence challenges ahead. 1–3 (2008)

[11] Boulares, S.: Validation des politiques de sécurité par rapport aux modèles de contrôle d'accès. Mémoire (MSc), Université du Québec en Outaouais, Département d'informatique et d'ingénierie (2010)

[12] Boulares, S., Adi, K. Logrippo, L.: Information flow-based security levels assessment for access control systems. E-Technologies. 105–121 (2015)

[13] Boulares, S., Adi, K. Logrippo, L.: Insider Threat Likelihood Assessment for Access Control Systems: Quantitative Approach. 9th International Symposium on Foundations & Practice of Security. 135-142 (2016)

[14] Boulares, S., Adi, K. Logrippo, L.: Insider Threat Likelihood Assessment for Flexible Access Control. E-Technologies. 77-95 (2017)

[15] Brewer, D. F., Nash, M. J.: The chinese wall security policy. IEEE Symposium on Security and Privacy. 206–214 (1989)

[16] Byun, J.-W., Li, N.: Purpose based access control for privacy protection in relational database systems. VLDB Journal. 17. 603–619 (2008)

[17] Cappelli, D., Moore, A., Trzeciak, R., Shimeall, T. J.: Common Sense Guide to Prevention and Detection of Insider Threats. Technical report, CERT Insider Threat Study Team. (2008)

[18] Chari, S., Lobo, J., Molloy, I.: Practical risk aggregation in RBAC models. 17th ACM symposium on Access Control Models and Technologies. 117–118 (2012)

[19] Chen, L., Crampton, J.: Risk-aware role-based access control. Security and Trust Management. 140–156 (2012)

[20] Cheng, P. C., Rohatgi, P., Keser, C., Karger, P. A., Wagner, G. M, Reninger, A. S.: Fuzzy multi-level security: An experiment on quantified risk-adaptive access control. IEEE Symposium on Security and Privacy. 222–230 (2007)

[21] Clusif.: La gestion des incidents de sécurité de l'information. Dossier technique. (2011)

[22] Clusif.: La gestion des risques - Concepts et méthodes. Dossier technique (2009)
[23] Clusif.: MEHARI 2010 Principes fondamentaux et spécifications formelles. Dossier technique. (2010)
[24] Cosquer, H.: Abus et détournements du secret-défense. Editions L'Harmattan, Paris. (2007)
[25] Covington, M. J., Moyer, M. J., Ahamad, M.: Generalized role-based access control for securing future applications. 23rd National Information Systems Security Conference. (2000)
[26] Crampton, J., Leung, W., Beznosov, K.: The secondary and approximate authorization model and its application to Bell-LaPadula policies. 11th ACM symposium on Access Control Models and technologies. (2006)
[27] Denning, D. E.: A lattice model of secure information flow. Communications of the ACM. 19. 236–243 (1976)
[28] Dershowitz, N., Manna, Z.: Proving termination with multiset orderings, Communications of the ACM. 22. 465–476 (1979)
[29] Diep, N. N., Hung, L. X., Zhung, Y., Lee, S., Lee, Y.-K. Lee, H.: Enforcing access control using risk assessment. 4th European Conference on Universal Multiservice Networks. (2007)
[30] Dimmock, N., Belokosztolszki, A., Eyers, D., Bacon, J., Moody, K.: Using trust and risk in role-based access control policies. 9th ACM symposium on Access control models and technologies. (2004)
[31] Farkas, C. The Inference Problem in Databases. Ph.D. Dissertation, Information Technology, George Mason University. (2000).
[32] Farkas, C, Jajodia, S. The Inference Problem: A Survey. SIGKDD Explorations. 6-11 (2002).
[33] Farkas, C. Toland, T, Eastman, C. The Inference Problem and Updates in Relational Databases. 15th IFIP WG11.3 Working Conference on Database and Application Security. 181-194 (2001).
[34] Ferraiolo, D., Cugini, J., Kuhn, D. R.: Role-based access control (RBAC): Features and motivations. 11th annual computer security applications conference. (1995)
[35] Ferraiolo, D., Kuhn, D. R., Chandramouli, R.: Role-based access control. Norwood (USA): Artech House. (2003).
[36] Ferraiolo, D. F., Sandhu, R., Gavrila, S., Kuhn, D. R., Chandramouli, R.: Proposed NIST standard for role-based access control. ACM Transactions on Information and System Security. 4, 224–274 (2001)
[37] FIPS.: PUB. 199. Standards for Security Categorization of Federal Information and Information Systems 2 (2004)
[38] FIPS.: PUB. 200. Minimum Security Requirements for Federal Information and Information Systems (2006)
[39] Fokoue, A., Srivatsa, M., Rohatgi, P., Wrobel, P., Yesberg, J.: A decision support system for secure information sharing. 14th ACM symposium on Access control models and technologies. (2009)
[40] Foley, S et al. Multilevel security and quality of protection. Quality of Protection. 93-105 (2006).
[41] Fouad, M. R., Lebanon, G., Bertino, E.: ARUBA: A risk-utility-based algorithm for data disclosure. Secure Data Management. 32 – 49 (2008)
[42] Friche, P.: Logiciels Open Source: introduction à Easy PHP et PMB. (2004)
[43] Galvin, P. B., Gagne, G., Silberschatz, A.: Operating system concepts. John Wiley & Sons, Inc. (2013)
[44] Gay, O. : Exploitation avancée de buffer overflows. Département d'Informatique de l'EPFL, Lausanne (2002)
[45] Granger, S.: Social engineering fundamentals, part I: hacker tactics. Security Focus. (2001)
[46] Han, W., Ni, Q., Chen, H.: Apply measurable risk to strengthen security of a role-based delegation supporting workflow system. IEEE International Symposium on Policies for Distributed Systems and Networks. (2009)

[47] Harrison, M. A., Ruzzo, W. L., Ullman, J. D.: Protection in operating systems. Communications of the ACM. 19. 461–471 (1976)
[48] House Committee on Government Operations: Executive Classification of Information--Security Classification Problems Involving Exemption (b) (1) of the Freedom of Information Act (5 U.S.C.552). House Report, U.S. Government Publishing Office (1973)
[49] Hu, J., Li, R., Lu, Z., Lu, J., Ma, X.: RAR: A role-and-risk based flexible framework for secure collaboration. Future Generation Computer Systems. 27. 574–586 (2011)
[50] Hu, V. C., Ferraiolo, D., Kuhn, D. R.: Assessment of access control systems. US Department of Commerce, NIST. (2006)
[51] Hu, V. C., Ferraiolo, D., Kuhn, R., Schnitzer, A., Sandlin, K., Miller, R., Scarfone, K.: Guide to attribute based access control (abac) definition and considerations. NIST Special Publication 800-162. (2014)
[52] IBM Thomas J. Watson Research Center.: System S: Appliction Areas, System and components, Programming Model. (2000)
[53] ISO/IEC.: ISO/IEC 31000 - Management du risque -- Principes et lignes directrices. (2009)
[54] ISO/IEC.: ISO/IEC 73 - Management du risque – Vocabulaire. (2009)
[55] ISO/IEC.: ISO/IEC 13335 - Management of information and communications technology security--Part 1: Concepts and models for information and communications technology security management. (2004)
[56] ISO/IEC.: ISO/IEC 27001 Systèmes de management de la sécurité de l'information – Exigences. (2013)
[57] ISO/IEC.: ISO/IEC 27005 - Gestion des risques liés à la sécurité de l'information. (2011)
[58] ISO/IEC.: ISO/IEC Guide 73 - Management du risque -- Vocabulaire -- Lignes directrices pour l'utilisation dans les normes. (2002)
[59] Kandala, S., Sandhu, R., Bhamidipati, V.: An attribute based framework for risk-adaptive access control models. 6th International Conference on Availability, Reliability and Security. 236–241 (2011)
[60] Khambhammettu, H., Boulares, S., Adi, K., Logrippo, L.: A framework for risk assessment in access control systems. Computers & Security. 39. 86–103 (2013)
[61] Khambhammettu, H., Boulares, S., Adi, K., Logrippo, L.: A Framework for Threat Assessment in Access Control Systems. IFIP Advances in Information and Communication Technology. 376, 187–198 (2012)
[62] Krautsevich, L., Martinelli, F., Morisset, C., Yautsiukhin, A.: Risk-based auto-delegation for probabilistic availability. Data Privacy Management and Autonomous Spontaneus Security. 206–220 (2012)
[63] Kaspersky Lab ZAO.: Global Corporate IT Security Risks. (2013)
[64] Lampson, B. W.: Protection. ACM SIGOPS Operating Systems Review. 8. 18–24 (1974)
[65] Landwehr, C. E.: Formal models for computer security. ACM Computing Surveys.13. 247 – 278 (1981)
[66] Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., Leaf, D.: NIST cloud computing reference architecture. NIST special publication 500. (2011)
[67] Logrippo, L.: Logical method for reasoning about Access Control and Data Flow Control models. Foundations and Practice of Security. 205–220 (2015)
[68] McCullough, D.: Covert channels and Degrees of Insecurity. Proc. of the computer security foundations workshop. (1988)
[69] McGraw, R.: Risk adaptive access control (RADAC). NIST Privilege management workshop. (2009)
[70] Ministère de la Justice Canadien.: Loi sur la protection des renseignements personnels, L.R.C. (1985)

[71] MITRE Corporation.: Broader Access Models for Realizing Information Dominance, Technical report JSR-04-132. (2004)
[72] Molloy, I., Cheng, P.-C., Rohatgi, P.: Trading in risk: Using markets to improve access control. 2008 workshop on New security paradigms. 107–125. (2009)
[73] Molloy, I., Dickens, L., Morisset, C., Cheng, P.-C., Lobo, J., Russo, A.: Risk-based security decisions under uncertainty. 2nd ACM conference on Data and Application Security and Privacy. 157–168. (2012)
[74] Myers, A. C., Liskov, B. Protecting privacy using the decentralized label model. ACM Transactions on Software Engineering and Methodology (TOSEM), 9(4). 410-442 (2000)
[75] National Association of Certified Fraud Examiners and United States of America.: Report to the Nation on Occupational Fraud and Abuse. (1996)
[76] National Computer Security Center.: Glossary of Computer Security Terms, NCSC- TG-004. (1988)
[77] Ni, Q., Bertino, E., Lobo, J.: Risk-based access control systems built on fuzzy inferences. 5th ACM Symposium on Information, Computer and Communications Security. 250–260 (2010)
[78] Nissanke N., Khayat, E. J.: Risk Based Security Analysis of Permissions in RBAC. 2nd International Workshop on Security In Information Systems. 332–341 (2004)
[79] OWASP.: OWASP Risk Rating Methodology.
[80] Park, J., Sandhu, R.: The UCON ABC usage control model. ACM Transactions on Information and System Security. 7. 128–174 (2004)
[81] Randazzo, M. R., Keeney, M., Kowalski, E., Cappelli, D., Moore, A.: Insider threat study: Illicit cyber activity in the banking and finance sector. DTIC Document, Technical report CMU/SEI-2012-SR-004, Software Engineering Institute. (2004)
[82] Samarati P., de Vimercati, S. C.: Access control: Policies, models, and mechanisms. Foundations of Security Analysis and Design. 137–196 (2001)
[83] Sandhu, R. S.: Lattice-based access control models. IEEE Computer. 26. 9–19 (1993)
[84] Sandhu, R. S., Coyne, E. J., Feinstein, H. L., Youman, C. E.: Role-based access control models. IEEE Computer. 29. 38–46 (1996)
[85] Sandhu, R. S., Jajodia, S.: Data and database security and controls. Handbook of Information Security Management. 481 – 499 (1993)
[86] Schultz, E. E.: A framework for understanding and predicting insider attacks. Computers & Security. 21. 526–531 (2002)
[87] Shay, H.: Understand the State of Data Security and Privacy: 2013 to 2014. Forrester Research Inc. (2013)
[88] Sklar, D.: Introduction à PHP 5. O'Reilly Media Inc. (2004)
[89] Srivatsa, M., Agrawal, D., Reidt, S.: A metadata calculus for secure information sharing. 16th ACM conference on Computer and communications security. 488– 499 (2009)
[90] Stoneburner, G., Goguen, A., Feringa, A.: NIST Special Publication 800-30, Risk management guide for information technology systems. (2002)
[91] Stine, K., Rich, K., Barker, C., Fahlsing, J., Gulick, J.: NIST SP. 800-60 Rev 1. Guide for Mapping Types of Information and Information Systems to Security Categories. (2008)
[92] Sun, Y., Li, N., Bertino, E.: Proactive defense of insider threats through authorization management. International workshop on Ubiquitous affective awareness and intelligent interaction. 9–16 (2011)
[93] US Department of Defense. Information security program.: DOD Manual, 5200.1-R. (1997)
[94] Varadharajan V., Black, S.: A multilevel security model for a distributed object-oriented system. 6th Annual Computer Security Applications Conference. 1–9 (1990)
[95] Wang, H., Zhang, Y., Cao, J.: Ubiquitous computing environments and its usage access control. 1st international conference on Scalable information systems. (2006)

[96] Wang, Q., Jin, H.: Quantified risk-adaptive access control for patient privacy protection in health information systems. 6th ACM Symposium on Information, Computer and Communications Security. 406–410 (2011)
[97] Wei, Q., Crampton, J., Beznosov, K., Ripeanu, M.: Authorization recycling in RBAC systems. 13th ACM symposium on Access control models and technologies. 63–72. (2008)
[98] Weissman, C.: Security controls in the ADEPT-50 time-sharing system. The Fall Joint Computer Conference. 119 – 133 (1969)
[99] Willison, R.: Understanding the perpetration of employee computer crime in the organisational context. Information and organization. 16, 304–324 (2006)
[100] Willison, R., Backhouse, J.: Opportunities for computer crime: considering systems risk from a criminological perspective. European journal of information systems. 15. 403–414 (2006)
[101] Wood, B.: An insider threat model for adversary simulation. SRI International, Research on Mitigating the Insider Threat to Information Systems. 1–3 (2000)
[102] J. Wray.: An Analysis of Covert Timing Channels. IEEE symposium on security and privacy. (1991)
[103] Zhang, G., Parashar, M.: Context-aware dynamic access control for pervasive applications. Communication Networks and Distributed Systems Modeling and Simulation Conference. 21–30 (2004)
[104] Zhang, L., Brodsky, A., Jajodia, S.: Toward information sharing: Benefit and risk access control (BARAC). Seventh IEEE International Workshop on Policies for Distributed Systems and Networks. 45–53 (2006)