Sécurisation d'une plate-forme dédiée à l'Intelligence Economique

Anass EL HADDADI *' -- Bernard DOUSSET* -- Ilham BERRADA****

** Institut de Recherche en Informatique de Toulouse, IRIT-SIG*
Université Paul Sabatier, 118 route de Narbonne, 31062 Toulouse cedex 9 (France)
haddadi@irit.fr – dousset@irit.fr

*** Equipe EL BIRONI, ENSIAS*
B.P. 713 Agdal – Rabat, Maroc
iberrada@ensias.ma

RÉSUMÉ. *Dans cet article nous présentons une démarche de sécurisation de notre plate-forme d'Intelligence Economique dédiée aux applications Mobile/Web, et ce, pour la protection des données sensibles qui proviennent des différentes analyses que nous effectuons. Pour ce faire, nous développons une ontologie spécifique pour la gestion de la sécurité des accès à la plate-forme, sachant que le réseau est ouvert et que les données stratégiques diffusées ne doivent être lues et manipulées que par des personnes autorisées.*

ABSTRACT. *In this paper, we present an approach to securing our Mobile/Web platform dedicated to the competitive Intelligence, in order to protect sensitive data resulting from the different studies and analyses that we provide. To do so, we develop a specific ontology that help us to manage security access to the platform.*

MOTS-CLÉS : *Ontologie de sécurité, intelligence économique, réseau de télécommunication.*

KEYWORDS: *Security Ontology, competitive intelligence, telecommunication network.*

1. Introduction

Les techniques d'analyse multidimensionnelle sont actuellement bien maîtrisées pour toutes les données quantitatives disponibles sur les systèmes d'information des entreprises ou des administrations à condition que le SGBD s'y prête, que le schéma de la base soit adapté et que les données soient de qualité (homogènes, actualisées, complètes, compatibles, à la bonne granularité, …). D'autre part, il est toujours possible d'extraire les données utiles vers une base de données construite sur mesure pour la fouille multidimensionnelle, en réalisant, au passage, toutes les corrections nécessaires à son exploitation. Par contre, pour le traitement des données textuelles issues de l'ensemble des sources électroniques, ce type d'analyse est difficile à mettre en place : les données sources ne sont pas au même format ou sont même non structurées, elles sont réparties, hétérogènes et la multitude des cas rencontrés ne permet pas de trouver une structure universelle où les regrouper. Afin d'unifier la fouille multidimensionnelle sur les données textuelles de toutes provenances, nous avons proposé une structure unique permettant de stocker toutes les relations inter items rencontrées dans les documents à analyser. Cette approche permet de construire des cubes croisant deux variables quelconques et le temps. Dès 2001, un premier outil XPlor a ainsi été proposé pour mettre en ligne ce type de structure en mode client serveur, afin de réaliser une fouille personnalisée via divers outils de restitution graphique des résultats. Toutes les données textuelles sont alors dans une même structure et bénéficient donc d'outils communs d'investigation interactive.

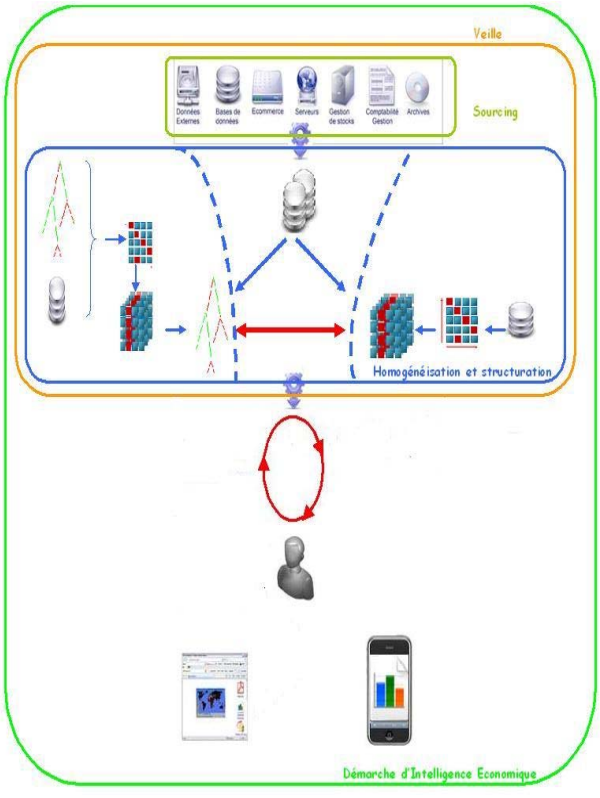

Figure 1. *Démarche d'Intelligence Economique*

Actuellement, nous envisageons le développement d'un Portail Web pour Mobile, afin de permettre aux utilisateurs de nos solutions de veille de continuer à rechercher, surveiller, valider et rediffuser des informations stratégiques au cours de leurs déplacements. Ils n'ont ainsi plus besoin

d'être assis face à leur ordinateur pour accéder à des données utiles dans l'instant (préparation d'une réunion, nouvel ordre du jour, information sur un interlocuteur, une technologie, un marché, demande urgente d'une analyse ou d'un focus spécifique). Il leur suffit simplement d'utiliser, où qu'ils se trouvent, leur appareil mobile de type iPhone. Grâce à ce « Portail Web Mobile », ils peuvent être en permanence au cœur de l'information pertinente.

Notre Portail Web pour Mobile se base sur les ontologies de domaines (El haddadi, 2009), sur les réseaux d'acteurs et sur une gestion de la sécurité elle-même contrôlée par une ontologie spécifique (Fig. 2).

Il est alors possible de :

Consulter des informations à jour, car nous accédons à notre serveur de base de donnée stratégique en temps réel, lui-même alimenté quotidiennement par des veilleurs.

Faire remonter des informations « terrain » lors de salons, de visites en clientèle ou à l'issue de réunions.

Demander des renseignements spécifiques en urgence qui seront mis en ligne par les veilleurs.

Réaliser des focus sur mesure à partir des sujets mis en ligne sur le serveur.

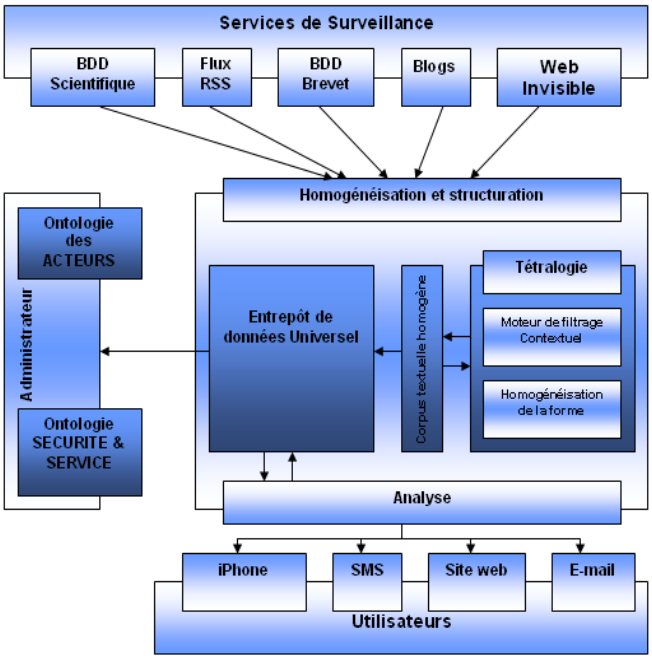

Figure2. *Architecture de la plate-forme d'IE*

Grâce à l'évolution de la technologie, un tel portail pour mobile doit nous permettre de gagner en efficacité et en réactivité car, à tout moment, il est possible d'accéder à toutes les informations stratégiques utiles au décideur nomade, lui-même pouvant faire remonter très vite l'information « terrain », qui peut éventuellement venir déclencher d'autres analyses stratégiques.

Cependant, l'un des problèmes majeurs est la protection des données sensibles. Ainsi, pour obtenir un niveau de sécurité satisfaisant sur un réseau de Télécommunication, il est nécessaire de connaître les vulnérabilités inhérentes à ce type de réseau, et de développer une ontologie spécifique pour la gestion de la sécurité.

2. Perspective de sécurisation de la plate forme d'IE

La mobilité c'est l'avenir des systèmes informatiques, puisque les appareils mobiles pénètrent progressivement notre société et notre mode de vie. Cependant, ces appareils possèdent des ressources faibles et leur média est entièrement contrôlé par les opérateurs. De plus, les applications mobiles sont suspectées d'être ouvertes à de nouvelles menaces et attaques. Il est donc vital de se concentrer sur l'aspect « sécurité » dans le domaine de la mobilité.

La sécurité, dans un tel contexte, peut être abordée par un classement des vulnérabilités et la définition des liaisons entre les services de sécurité. Dans l'objectif de protéger les données stratégiques, nous envisageons de suivre la démarche suivante :

Identification des objets à sécuriser. Afin d'identifier sans ambigüité et avec exhaustivité tous les objets à sécuriser, il est nécessaire de modéliser la plate-forme toute entière et donc son workflow.

Mise en place de la politique de sécurité de la plate-forme : Comme la plate-forme d'IE se base principalement sur des concepts, nous envisageons, par souci de cohérence, de mettre en place une « Ontologie de Sécurité ». Cette ontologie doit contenir les éléments suivants :

- Les différents intervenants ou acteur qui interagissent avec la plate-forme.
- Les types d'opérations que peut exécuter chaque acteur (les cas d'utilisations).
- Les différents droits d'accès ou d'exécution d'une opération (permission, obligation, déni).

3. Les sources de sécurité pour les applications mobiles

D'après (ISO 7498-2, 1989) les services de sécurité sont : authentification, contrôle d'accès, non répudiation, intégrité et confidentialité. Pour mettre en œuvre, déployer et utiliser les services mentionnés, nous devons utiliser différents mécanismes. Selon le sondage de (Beji, 2009), le tableau suivant nous donne une description de sécurité selon le type d'acteur.

Auteur	Description	Exemples
Périphérique de la Plate-forme	Toutes les fonctionnalités de chiffrement, fonction de hachage, de gestion des clés	API JME de sécurité
La carte à puce : SIM1, UICC2	Quelque fonctionnalité de chiffrement, hachage, clé de stockage.	API Javacard de sécurité
Protocoles et schémas	Les protocoles de sécurité existants, tels que l'échange de clés, les schémas d'authentification	Changement de clés Diffie-Hellmen3
Fournisseur de contenu	Le contenu doit être protégé contre la copie ou le trafic à partir de son fournisseur.	Gestion des droits d'accès.
Opérateur télécom	L'opérateur télécom doit contribuer à l'authentification et l'autorisation.	Distribution de certificats, signature de code
Fonctionnalité des périphériques physiques	Selon le périphérique, certaines fonctionnalités de sécurité doivent être disponibles.	Biométrie, authentification, mémoire de verrouillage.

Table 1. *Les sources de sécurité pour les applications mobiles (Beji, 2009)*

4. L'assurance de sécurité : exigence d'une ontologie

En raison de la diversité des acteurs, des rôles, et des contraintes, des temps d'exécution, des tâches complexes de la sécurité, un modèle de base de connaissance doit être utilisé pour exprimer ces conditions. Ces solutions sont adaptées à un usage spécifique. Ce que nous ciblons c'est le partage et la fourniture

1 Subscriber Identity Module

2 Universal Integrated Circuit Card

33 En cryptographie, l'échange de clés Diffie-Hellman, du nom de ses auteurs Whitfield Diffie et Martin Hellman, est une méthode par laquelle deux personnes nommées conventionnellement Alice et Bob peuvent se mettre d'accord sur un nombre (qu'ils peuvent utiliser comme clé pour chiffrer la conversation suivante) sans qu'une troisième personne appelée Ève puisse découvrir le nombre en écoutant.

des concepts qui seront utilisés de façon constante à travers notre plate-forme Mobile d'IE.

Un patron de connaissance formelle des concepts de la sécurité mobile nous fournit une base solide pour proposer une approche applicable aux plates-formes Web-Mobile. C'est pour cette raison que nous avons adopté le formalisme des ontologies pour exprimer la connaissance requise dans le domaine de la sécurité mobile.

5. Présentation de l'ontologie

L'ontologie de sécurité a un double objectif : tout d'abord la mise en place d'une connaissance formelle sur la sécurité dans le cadre des applications mobiles, puis l'identification des contre-mesures possibles qui devrait être appliquées pour la sécurisation de notre plate-forme d'IE.

Dans la mesure du possible, nous essayons de répondre aux questions suivantes :

Q1 : Quels sont les mécanismes associés aux services de la sécurité dans le domaine du mobile ?

Q2 : Quels sont les mécanismes offerts par chacun des acteurs ?

Q3 : Quelles sont les technologies utilisées pour mettre en œuvre un mécanisme ?

Q4 : Quelles sont les relations entre la sécurité et d'autres exigences non fonctionnelles ?

Q5 : Quels sont les mécanismes qui devraient être utilisés pour atténuer une menace ?

Les ontologies de sécurité sont nombreuses dans la littérature (Herzog, 2007) (Kim, 2005) (Raskin, 2001) (Ahmed, 2007), chacune est définie pour un type spécifique d'utilisation. Les importations et la réutilisation sont les bases du partage des connaissances pour les ontologies, en fait, nous avons partiellement fondé notre ontologie sur les travaux de Herzog, Shahmehri et la Douma (Herzog, 2007), qui traitent de la sécurité des systèmes d'information, ainsi que sur les travaux de Beji et El Kadhi (Beji, 2009) qui proposent une ontologie de sécurité pour les applications mobiles.

(Beji, 2009) ont décrit les concepts et les relations les plus significatifs dans le domaine : de la vulnérabilité, des menaces, des biens, des contraintes, des acteur, des mécanisme, des ressources et des services. Leur proposition est sémantiquement composée de trois sous-ontologies :

Actif-Vulnérabilité-Threat Ontology (AVTO).

Mobile Profile Ontology (MPO)

Defense Mechanism Ontology (DMO)

La Fig. 3 donne une vue d'ensemble de l'ontologie principale avec certaines relations entre les sous-ontologies proposées par (Beji, 2009). Ces auteurs ont fait cette distinction, afin de permettre la réutilisation et le partage.

Le MPO définit les fonctionnalités d'utilisation possibles avec les ressources associées Fig.4. Tels que chaque mobile utilise certaines ressources, la construction de MPO se base sur une classification des ressources disponible pour les différents cas d'utilisations.

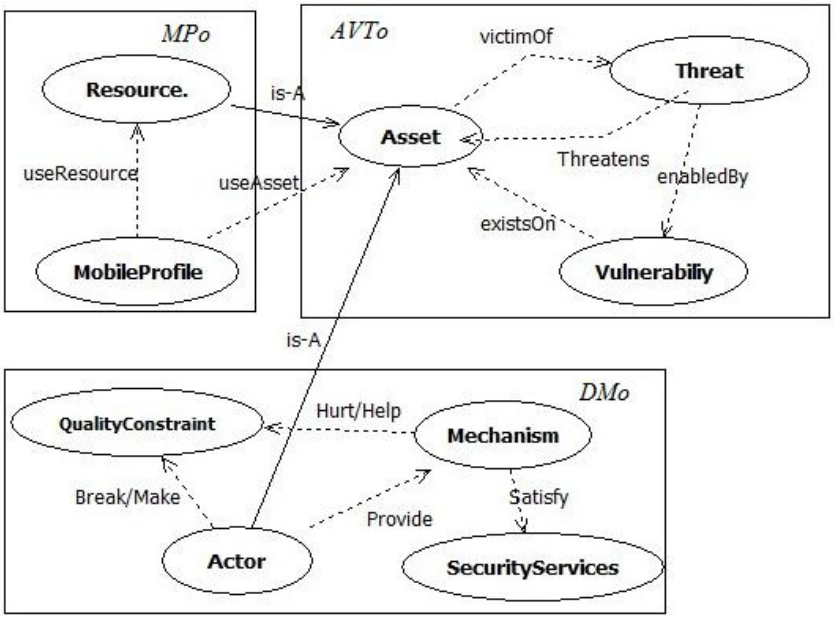

Figure 3. *L'ontologie de sécurité (Beji, 2009)*

La gestion Vulnérabilité-Menace est largement adaptée à une sous-ontologie (AVTO), où les classes supérieures et les relations principales sont les mêmes et seulement les sous-classes des vulnérabilités diffèrent d'un contexte à un autre. Notre objectif est l'enrichissement de cette sous-ontologie avec des vulnérabilités particulières, pour la protection des données stratégiques.

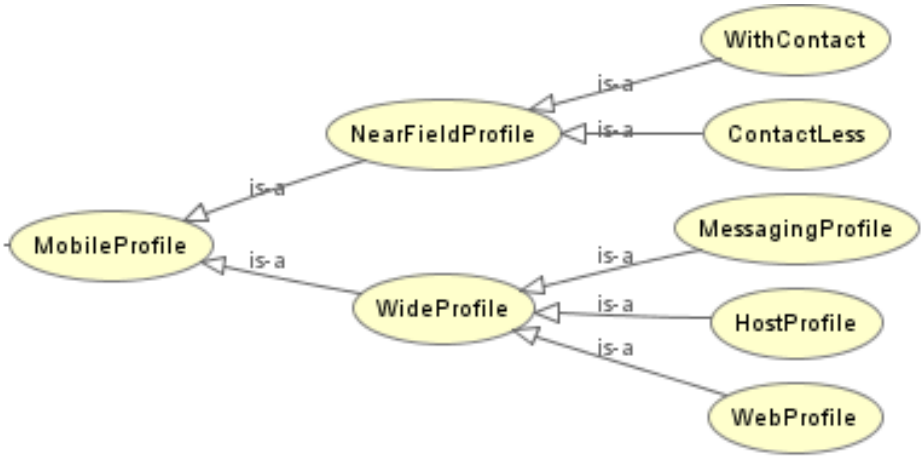

Figure 4. *Ontologie des technologies mobile (Beji, 2009)*

Enfin, le DMO gère les services de sécurité et les mécanismes de sécurité associés.

4. Identification de services de sécurité

En raison de la diversité des acteurs (Documentaliste, Analyste, Décideur, Membre) et des rôles (Ajouter une analyse, valider une analyse, etc.), nous sécurisons les différents types d'opérations que peut exécuter chaque acteurs, en se basant sur les diagrammes des cas d'utilisations[4].

En fait, selon l'approche proposée par (Supakkul, 2005), le méta-modèle de cas d'utilisation contient 4 méta-éléments qui sont, acteur, cas d'utilisation, association entre acteur et cas d'utilisation et enfin système. Pour ces éléments, nous devrons définir les exigences de sécurité associées. Par exemple, dans la Fig. 5, la validation d'une analyse stratégique a besoin de trois services de sécurité : la confidentialité, l'intégrité et la non répudiation. A l'aide de cette approche, on peut définir les services de sécurité nécessaires à chaque cas d'utilisation.

4 En UML (*Unified Modeling Language*), les diagrammes de Cas d'Utilisation (Use Case) constituent le moyen essentiel pour saisir les fonctionnalités d'un système du point de vue de l'utilisateur et remplacent souvent le cahier des « besoins fonctionnels ».

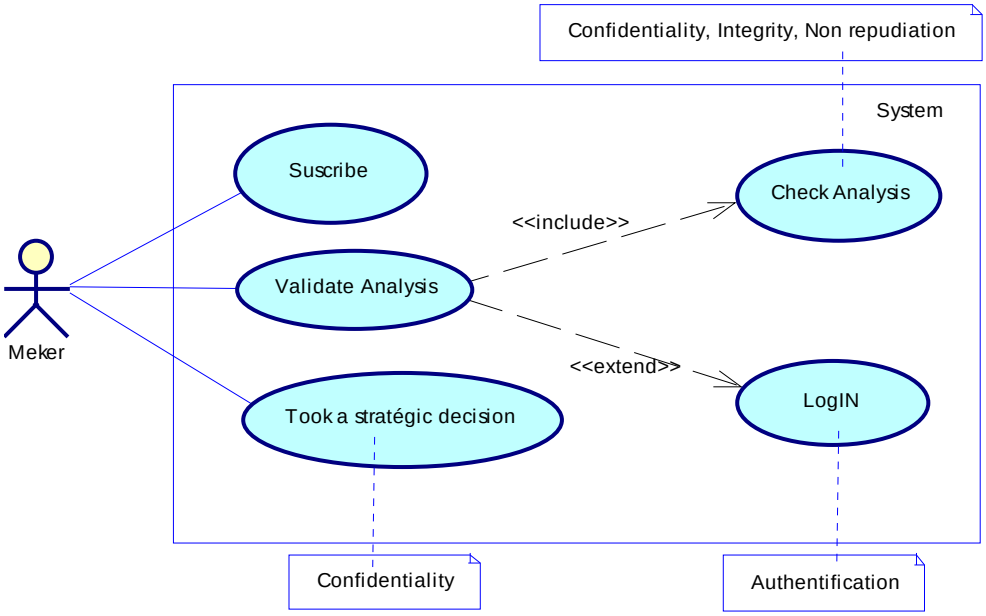

Figure 5. *Service de sécurité pour un cas d'utilisation*

6. Conclusion

L'exigence de sécurité pour notre plate forme d'IE consiste à acquérir toutes les connaissances et les technologies disponibles pour la conception et le déploiement de politiques de sécurité fiables et utilisables. Nous proposons dans cet article, une solution via les bases de connaissances grâce à la conception d'une ontologie de sécurité. En se basant, sur trois ontologies MPO, DMO et AVTO, puis nous introduisons les services de sécurités nécessaires à chaque cas d'utilisations.

Le déploiement de l'approche sécuritaire proposée, nous permet de sécuriser :

- Les opérations que peuvent exécuter les différents intervenants ou acteurs qui interagissent avec la plate-forme.
- Les données stratégiques et/ou confidentielles.

Durant nos prochains travaux, nous envisageons d'améliorer l'ontologie proposée. En mettant à jour, les concepts, les profils des utilisateurs, les droits d'accès, avant de diffuser toute information stratégique.

7. Bibliographie

Ahmed M., Anjomshoaa A., Nguyen T. M., Min T. A, « Towards an Ontology-based Organizational Risk Assessment in Collaborative Environments Using the SemanticLIFE », International Conference on Availability, Reliability and Security, ARES 2007.

Beji S., El Kadhi N., « Security ontology proposal for mobile applications », International Conference on Mobile Data Management: systems, Services and Middleware, pages: 580-587, 2009.

El haddadi A., Dousset B., Berrada I., Kassou I., « Construction d'une ontologie de domaine fondée sur le text mining », colloque Veille Stratégique et technologique, 2009.

Herzog A., Shahmehri N., Duma C., « An Ontology of Information Security » , International Journal of Information Security and Privacy, Volume 1, Issue 4, 2007.

ISO 7498-2: Information Processing Systems—Open System Interconnection—Basic Reference Model – Part 2: Security Architecture, 1989.

Kim A., Luo J., Myong K., « Security Ontology for Annotating Resources », LNCS 3761, pp. 1483 – 1499. Springer-Verlag Berlin Heidelberg 2005.

Raskin V., Hempelmann C. F., Triezenberg K. E., Nirenburg S., « Ontology in Information Security: A Useful Theoretical Foundation and Methodological Tool », Proceedings of the 2001 workshop on New security paradigms, Cloudcroft, New Mexico, Pages: 53-59.

Supakkul S., Chung L., « A UML Profile for Goal- Oriented and Use Case-Driven Representation of NFRs and FRs » , Proceedings of the 2005 Third ACIS Int'l Conference on Software Engineering Research, Management and Applications (SERA'05), 2005, IEEE.