Vers une nouvelle génération de définition des exigences de sécurité fondée sur l'utilisation des ontologies

Amina Souag

Vers une nouvelle génération de définition des exigences de sécurité fondée sur l'utilisation des ontologies

Amina Souag

CRI Paris 1 / ISID CNAM
90 rue de Tolbiac,
75013 Paris - France
Amina.Souag@malix.univ-paris1.fr

RÉSUMÉ. *Au cours de ces dernières années, la sécurité des Systèmes d'Information (SI) est devenue une préoccupation importante, qui doit être prise en compte dans tous les phases de développement du SI, y compris dans la phase initiale de l'ingénierie des exigences (IE). Des études récentes proposent quelques approches utiles pour la définition des exigences de sécurité. Cependant les analystes continuent de souffrir d'un manque important de connaissances sur la sécurité et sur le domaine d'activité des entreprises. Les ontologies sont connues pour être des sources riches de ces connaissances . Nous proposons, dans cette recherche, de mobiliser des ontologies dans le processus d'ingénierie des exigences. Nous voulons montrer que le recours à des ontologies pour supporter ce processus est un facteur clé de succès dans la définition d'exigences de sécurité de haute qualité.*

ABSTRACT. *During recent years, security in Information Systems (IS) has become an important issue, and needs to be taken into account in all stages of IS development, including the early phase of Requirement Engineering (RE). Recent studies proposed some useful approaches for security requirements definition but analysts still suffer from a considerable lack of knowledge about security and domain field. Ontologies are known to be wide sources of knowledge. We propose in this research to use ontologies to support the requirements engineering process. We aim to check that ontology-based security engineering is a key success factor to reach a security requirements elicitation of high quality.*

MOTS-CLÉS : *exigences de sécurité, ontologie de sécurité, ontologie de domaine, sécurité.*

KEYWORDS: *security requirements, security ontology, domain ontology, security.*

1. Introduction

L'un des défis auxquels les développeurs font face durant le développement des SI modernes est la sécurité de ces systèmes. Cette dernière, considérée comme préoccupation marginale au départ, traitée à une phase avancée du processus de développement, a complètement changé de statut (vu le nombre croissant des attaques). Elle devient une obligation importante à prendre en compte par toute l'entreprise. Les recherches récentes proposent de l'inclure dès les premières étapes d'analyse et de définition des exigences SI. Rappelons que la sécurité par définition est une discipline qui permet de construire des systèmes fiables qui font face aux accidents, erreurs ou malveillances (Giorgini *et al.,* 2004). La British Standards Institution la définit comme: "la protection des actifs face à un grand nombre de menaces " (BSI1, 1999) "qui sont d'origines diverses : accidentelles ou volontaires, naturelles, humaines ou techniques" (Claviez, 2002). Le concept de sécurité des SI recouvre aussi un ensemble de méthodes, techniques et outils chargés de protéger les ressources d'un SI afin d'assurer sa disponibilité, sa confidentialité, son intégrité et sa traçabilité (Glinz, 2007).

L'ingénierie des exigences est la science concernée par l'analyse et la documentation des exigences (Kauppinen *et al.*, 2002). Les exigences de sécurité incluent les types et niveaux de protection nécessaires pour les équipement, données, informations, applications et installations pour adaptés à la politique de sécurité. Les exigences de sécurité sont les traduction des demandes des prenantes du projet que certains actifs soit protégés de tout dommage. Elles veulent par exemple que les informations ne soient pas détruites, volées, ou modifiées. L'ingénieur chargé de la définition des exigences exprime les exigences de sécurité pour restreindre le nombre de cas où ces résultats négatifs peuvent avoir lieu. Un credo de longue date en l'ingénierie des exigences dit: " Si vous ne savez pas ce que vous voulez faire, c'est difficile de le faire juste" (Fabian *et al*., 2010). Cette assertion a une signification particulière pour les exigences de sécurité, puisque souvent, pour l'analyste il s'avère difficile de savoir au préalable quoi sécuriser ? contre qui ? à quel niveau ? Malgré les différentes approches existantes dans le domaine (section 3.2), la plupart des ingénieurs et analystes restent insuffisamment formés pour être en mesure de définir des exigences de sécurité. Ceci est dû à un manque important de connaissance d'une part en sécurité et d'autre part dans le domaine d'activité de l'entreprise (Firesmith, 2003).

Une ontologie, dans le domaine de la représentation des connaissances, est définie comme étant "une représentation d'une conceptualisation" (Gruber, 1995). Les ontologies sont utiles pour représenter et mettre en relation de nombreux types de connaissances. Les ontologies de domaines sont des descriptions formelles de classes de concepts et de relations entres ces concepts qui décrivent un domaine donné. La question que nous nous posons, est relative à l'utilité des ontologies pour la définition des exigences de sécurité ?

La suite de l'article est organisée comme suit : la 2éme section aborde la problématique de notre recherche. La section 3 présente la proposition, avec entres autre l'approche, les travaux connexes et les résultats attendus. Enfin la section 4 fait le point sur l'état d'avancement et les travaux futurs.

2. Problématique

Les exigences de sécurité sont connues pour être difficiles à identifier, à exprimer et à manager. En examinant les documents de spécification des exigences, nous constatons habituellement que les exigences de sécurité, quand elles figurent, sont dans une section à part et ont été recopiées à partir d'une liste générique de fonctions de sécurité. L'élucidation et l'analyse des exigences qui sont nécessaires pour obtenir un ensemble d'exigences de sécurité plus spécifique sont rarement effectuées. L'étude des approches de définition des exigences de sécurité et des notations de modélisation relatives à la sécurité (section 3.2), nous a permis d'en voir les limites pour le développement d'applications sécurisées. Une partie de ces approches (UMLSec et SecureUML) prennent en compte la sécurité à un niveau système et ne supportent pas la modélisation et l'analyse de la sécurité à un niveau organisationnel. Elles ont pour but de modéliser les systèmes informatiques et les mécanismes de contrôle d'accès associés et non les exigences de sécurité. Parfois, elles tendent à être partielles et ne modélisent pas tous les aspects de la sécurité. D'autres approches (Secure i* et Secure Tropos) traitent les problèmes de sécurité de façon générale et non pas pour un domaine donné. Le processus proposé pour la définition des exigences dans ces approches est incomplet ou n'existe même pas.

Par ailleurs, avec la nécessité croissante de mettre en oeuvre des mesures de sécurité dans un environnement donné, un obstacle majeur que rencontrent les analystes et les développeurs utilisant les approches de modélisation existantes, est le manque avéré de connaissance et d'expertise sur la sécurité et sur le domaine d'activité d'une entreprise. Des études récentes ont montré que le manque de connaissances en sécurité de l'information au niveau métier est l'une des raisons donnant lieu à des stratégies de gestion de la sécurité inadéquates ou non existantes, et qu'une sensibilisation à une meilleure gestion de la sécurité de l'information au niveau métier et une meilleure connaissance du domaine conduiront à des stratégies plus efficaces. Pour combler ces différentes lacunes, une grande partie des recherches et des développements applicatifs en ingénierie de la sécurité est dédiée au développement des ontologies et de bases de connaissances de sécurité. Plusieurs ontologies de sécurité ont été proposées (Souag *et al., 2012*). Elles varient de par leur degré de généralité (niveau métier) et de spécificité (niveau technique). Elles varient aussi dans leur couverture des aspects de sécurité. Certaines se concentrent plus sur les vulnérabilités, lorsque d'autres sont dédiées aux menaces, ou aux contre-mesures, etc. De plus, certaines ontologies de domaines existent dans la littérature, par exemple pour le domaine médical, bancaire, aéronautique et maritime.

Nous nous proposons d'explorer l'utilisation de ces ontologies (de domaine et de sécurité) pour définir une approche de guidage dans l'élucidation, l'analyse et la validation des exigences de sécurité. Comment ? Est-ce une solution intéressante pour couvrir certaines lacunes dans la définition d'exigences de sécurité complètes, consistantes et non ambiguës? sont les questions de recherches que nous nous posons. Nous souhaitons tester trois hypothèses principales : que (H1) la définition des exigences de sécurité peut être effectuée à l'aide d'une démarche en plusieurs étapes par analogie à la définition des exigences fonctionnelles, que (H2) les ontologies de sécurité et de domaine sont utile à chaque étape de la démarche, et que (H3) la méthode a définir sera meilleure que les méthodes existantes, notamment grâce à l'utilisation des ontologies.

3. Proposition

Comme mentionné dans la section 2, une étape a été parcourue dans le domaine de l'ingénierie des exigences de sécurité, en particulier dans les approches de modélisation et d'analyse des exigences, mais des questions importantes sont toujours ouvertes et doivent être prises en considération. En particulier, un réel manque de connaissance sur la sécurité et le domaine à différents niveaux de développement laissent ces propositions inutiles. Notre objectif est de tirer profit des ontologies de sécurité et de domaine existantes et de proposer des mécanismes et des techniques permettant de les utiliser au sein d'une approche de guidage pour la définition et l'analyse des exigences de sécurité pour un domaine d'activité.

3.1. *L'approche proposée*

L'approche proposée reprend les étapes de (Wiegers, 2003) pour le développement des exigences, mais les adapte pour la définition des exigences de sécurité. Nous exploitons l'utilisation des ontologies de sécurité et de domaine à chaque étape. La figure 1 donne une vue générale de l'approche proposée.

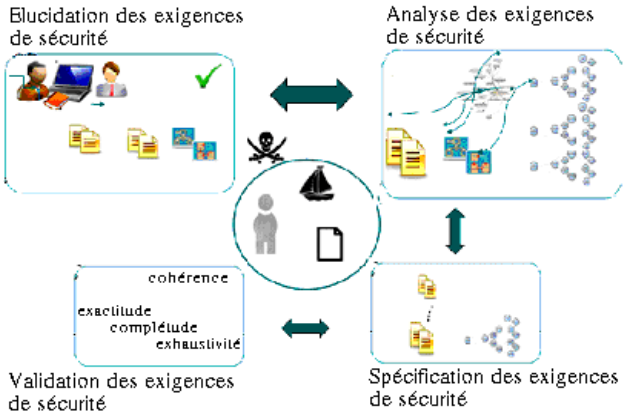

Figure 1. Le cadre de référence pour la définition des exigences de sécurité.

Au centre, on schématise le système d'information (SI) d'une entreprise donnée, caractérisé par ses dimensions humaine , physique et informationnelle (les actifs). Le SI est exposé à des menaces diverses qui exploitent des vulnérabilités dans le système. La figure représente, autour du SI, les quatre étapes (élucider , analyser , spécifier et valider) à suivre pour élaborer le document cible d'exigences de sécurité.

- *L'élucidation des exigences de sécurité :* En premier lieu, l'étape d'élucidation, au cours de laquelle les problèmes de sécurité sont identifiés, des interviews auprès des parties prenantes sur les besoins et les buts en termes de sécurité sont obtenus. Pour ce faire, nous suggérons d'utiliser des questionnaires, d'examiner les documents de sécurité du domaine (nomenclatures, réglementations, etc.), d'organiser des réunions avec les parties prenantes, mais aussi d'effectuer des visites afin d'effectuer des constats sur place. Identifier les acteurs, et surtout les acteurs malveillants potentiels, les vulnérabilités, les menaces, les actifs de l'entreprise, et imaginer certaines contre mesures. Le résultat de cette étape consiste en un premier ensemble d'exigences de sécurité textuelles, complété par un modèle des exigences correspondantes (en utilisant i* par exemple).

- *L'analyse des exigences de sécurité :* L'étape d'analyse vise à raffiner, restructurer et enrichir les exigences de sécurité recueillies au cours de l'étape précédente. Le but de cette étape est de compléter les exigences déjà identifiées en introduisant les ontologies. Elle contient plusieurs sous étapes : normaliser la terminologie, formaliser les exigences de sécurité, mapper le modèle d'exigences de sécurité avec les ontologies (grâce à des règles à définir) de manière à identifier les incomplétudes, identifier de nouvelles exigences. Recommencer ces étapes jusqu'à ce qu'il n'y ait plus d'incomplétude. Le résultat de cette étape sera: un indicateur d'incomplétude (par rapport aux ontologies), un modèle i* complet, des exigences identifiées mais non formalisées.

- *La spécification des exigences de sécurité :* La spécification consiste à documenter les exigences de sécurité d'une manière durable et efficace pour toutes les parties prenantes du projet (développeurs, testeurs, clients etc.). Ici encore, nous suggérons d'utiliser les ontologies : des ontologies générales de sécurité pour les exigences métiers, ainsi que des ontologies de sécurité techniques pour les exigences de sécurité.

- *La validation des exigences de sécurité :* Finalement, lors de la dernière étape, les parties prenantes revoient les exigences de sécurité. Puis elles sont testées au moyen d'un prototype. Enfin, une validation des attributs de qualité de ces exigences (cohérence, exactitude, exhaustivité, complétude) doit être menée, fondée sur le document des exigences de sécurité.

3.2. *Travaux connexes*

La communauté IE a pris conscience de l'importance de la sécurité dans les dernières années et beaucoup d'approches d'IE ont été développées : Il existe des

approches en IE d'analyse d'exigences de sécurité mais elles n'exploitent pas les ontologies: des approches orientées objet fondées sur des extensions UML, comme les profils UML (SecureUML (Lodderstedt *et al.*, 2002), UMLSec (Jürjens, 2002)), et les cas d'utilisation (Misuse Cases (Sindre *et al*. ,2004), Abuse Cases (McDermott *et al.*, 1999), Security Use Cases (Firesmith, 2003). Des approches orientées but et agent, comme i* étendu (Liu et al., 2003), KAOS étendu (Lamsweerde, 2007) et Tropos étendu (Moratidis, 2006). Il existe aussi des approches fondées sur l'analyse des risques (Hermann *et al.,* 2010) (Mayer *et al.*, 2005). Il existe des approches d'IE qui exploitent des ontologies, mais elles ne tiennent pas compte du rôle complémentaire des ontologies de sécurité et de domaine (Saeki *et al.*, 2006), (Liu et al., 2007).

A notre connaissance, aucune de ces approches n'a considéré l'utilisation à la fois des ontologies de domaine et de sécurité dans le processus de développement des exigences de sécurité. Ceci laisse la définition des exigences générique et incomplète et nécessite la participation des acteurs ayant des différentes compétences (SI, sécurité, domaine métier).

3.3. *Résultats attendus*

Ce travail de recherche a pour but de proposer une nouvelle approche évolutive et outillée, de guidage dans la définition des exigences de sécurité pour un domaine particulier. L'originalité principale réside dans l'utilisation de la connaissance extraites, des ontologies de sécurité et de domaine. L'approche va guider l'analyste concepteur en lui fournissant des ontologies, un outil et des mécanismes pour en extraire des éléments pertinents de connaissance afin de les appliquer à son analyse des exigences de sécurité. Le résultat visé est une meilleure définition des exigences de sécurité. Ainsi, nous nous attachons à définir 1) les étapes de la méthode 2) les éléments requis pour mener à bien chaque étape 3) les livrables liés à chaque étape 4) les règles de guidage pour l'analyste en charge de l'étape 5) les éléments de validation de la fin de chaque étape. Nous spécifierons ensuite le cahier des charges de l'outil support de la méthode pour lequel nous construirons un prototype. La méthode et l'outil seront validés au moyen d'une étude de cas maritime.

4. Etat d'avancement

Ce projet de recherche se situe à l'intersection de trois grands domaines : l'ingénierie des exigences, l'ingénierie de la connaissance et l'ingénierie de la sécurité. La méthodologie de recherche utilisée s'appuie sur (Hevner et Chatterjee 2010). La première étape a consisté à comprendre le domaine de la sécurité, en acquérir les bases par le recensement des différentes définitions. Ensuite, nous avons effectué deux états de l'art des recherches et propositions dans les deux domaines des exigences de sécurité et des ontologies de sécurité pour la définition des exigences.

Nous avons étudié la plupart des approches dédiées à la définition des exigences de sécurité (12 approches), nous les avons classées en trois familles (orienté objet, orienté agent et but , orienté analyse des risques), nous avons analysé comment chaque approche modélise les exigences de sécurité (concepts, processus, avantages et limitations). Nous avons étudié aussi de nombreuses d'ontologies de sécurité existantes (23) et les avons classées en huit familles (Souag *et al,*. 2012) De plus, nous avons étudié comment chaque ontologie couvre les aspects de sécurité, ainsi que l'éventuelle utilisation de l'ontologie pour la définition des exigences. Ce travail de bibliographie est toujours en cours. Comme mentionné dans la section 3.2, certaines contributions s'intéressent à des problèmes similaires, mais la bibliographie indique qu'il n'existe pas d'approche en cours qui ait pour but de couvrir globalement l'ensemble des étapes du processus.

Le domaine de l'ingénierie des exigences étant vaste et varié, nous nous sommes concentrer uniquement sur certains points d'intérêt. Nous avons étudié principalement les approches orientées buts, axées sur la modélisation des exigences de sécurité. Nous avons aussi considéré les ontologies génériques de la sécurité à ce stade. Nous avons exploré une étude de cas associée au domaine maritime. Nous avons mené des interviews avec des parties prenantes du domaine maritime. Un premier jet d'exigences de sécurité a été rassemblé, des modèles d'exigences ont été élaborés fondés sur les interviews et l'analyse de certains documents régissant la sécurité maritime. Nous sommes actuellement en train de tester l'incorporation des ontologies de sécurité dans le processus de définition des exigences en nous appuyant sur ce cas riche en termes de problématiques de sécurité. Nous nous appuierons sur le cas maritime pour valider l'utilité de la méthode et sur un prototypage pour valider sa faisabilité.

5. Remerciements

Je remercie mes deux encadrants Camille Salinesi et Isabelle Comyn Wattiau pour leur assistance et conseils dans ce projet. Ce travail est subventionné par une allocation ministérielle de recherche de l'université Paris 1 Sorbonne. Il est conduit conjointement avec les deux équipes du CRI Paris 1 et ISID-CEDRIC du CNAM.

6. Bibliographie

BS799-1: Information Security Management - Part 1: Code of Practice for Information Security. British Standards Institution, London. 1999.

Claviez Jacques, *Sécurité informatique* , Paris , J.C.i. Inc : 2002.

Fabian, Benjamin, Seda Gürses, Maritta Heisel, Thomas Santen, et Holger Schmidt. 2010. « A comparison of security requirements engineering methods ». *Requirements Engineering* .

Firesmith, Donald G., et Firesmith Consulting. 2003. « Engineering Security Requirements ». *Journal of Object Technology* 2: 53–68.

Firesmith Donald: "Security Use Cases", in *Journal of Object Technology*, May-June 2003.

Glinz, M. 2007. « On Non-Functional Requirements » . *RE '07*, 21 –26 India, 2007.

Giorgini P., Mouratidis, , Manson, G., 'Towards the development of secure information systems: Security Reference Diagram and Security Attack Scenarios' *Proceedings of the FORUM at International CAiSE', Riga – Latvia*, 2004.

Gruber, T. R., 'Toward Principles for the Design of Ontologies Used for Knowledge Sharing', *International Journal Human-Computer Studies*, , 1995.

Herrmann, Andrea and Morali, Ayse, RiskREP: Risk-Based Security Requirements Elicitation and Prioritization ,2010.

Hevner, Alan, et Samir Chatterjee. 2010. *Design Research in Information Systems: Theory and Practice*. 1er éd. Springer.

Jürjens Jan, "UMLsec: Extending UML for Secure Systems Development", *Proceedings of the 5th International Conference on The Unified Modeling Language*,2002.

Kauppinen M., Kujala S., Aaltio T. and Lehtola L., "Introducing Requirements Engineering: How to Make a Cultural Change Happen in Practice", *RE'* 2002.

Lamsweerde . "Engineering Requirements for System Reliability and Security", *Vol. 9. IOS Press,* 2007, 196-238.

Lodderstedt T., Basin D. Jürgen D., "SecureUML: A UML-Based Modeling Language for Model-Driven Security" , *Proceedings of the 5th International Conference on The Unified Modeling Language,*2002.

Mayer N., Rifaut A., Dubois E., "Towards a Risk-Based Security Requirements Engineering Framework", *(REFSQ'05)*, Porto, Portugal, June 2005.

Liu, L., Yu, E., Mylopoulos, J., "Security and Privacy Requirements Analysis within a Social Setting", *RE', Proceedings. 11th IEEE International*, 2003.

Liu Wei; He Ke-Qing; Wang Jiang; Peng Rong; "Heavywight Semantic Induxement for Requirement Elicitation and analysis",3rd ،*Semantics, Knowledge and Grid*, 2007.

McDermott J., Fox C., "Using Abuse Case Models for Security Requirements Analysis". *In Proc. of ACSAC'99*, pages 55–66. IEEE Press, 1999.

Mouratidis H., 'Analysing Security Requirements of information systems using Tropos', on *Enterprise Information Systems*, 2006.

Saeki Motoshi, Kaiya Haruhiko, "Using Domain Ontology as Domain Knowledge for Requirements Elicitation". *RE'* 2006.

Sindre, Guttorm, and Andreas L Opdahl. "Eliciting security requirements with misuse cases." *RE'* ,2004.

Souag Amina, Salinesi Camille, Isabelle Wattiau, "Ontologies for Security requirements : A Literature Survey and Classification", WISSE, CAiSE, Juin 2012.

Wiegers K. *Software Requirements*, Microsoft Press, 2003.