Une méthode de définition des exigences de sécurité fondée sur l'utilisation des ontologies.

Amina Souag

Doctorant (email) : Amina Souag (Amina.Souag@malix.univ-paris1.fr)
Directeurs de Thèse : Pr. Camille Salinesi & Pr. Isabelle Wattiau
Laboratoire, Université : Centre de Recherche en Informatique (CRI), Equipe ISID (CNAM)

Une approche structurée pour la définition des exigences de sécurité fondée sur les ontologies de sécurité et de domaine

Mots-clés : exigences de sécurité, ontologies, sécurité, élucidation, analyse.

Résumé :

Au cours de ces dernières années, la problématique de la sécurité (disponibilité, intégrité, confidentialité, traçabilité) des systèmes d'information est devenue une préoccupation importante, qui doit être prise en compte au plus tôt dans le cycle de développement des systèmes, et tout particulièrement dans la phase d'ingénierie des exigences (IE).
Plusieurs travaux ont déjà été menés sur l'ingénierie des exigences de sécurité. Différentes approches, utiles pour la définition des exigences de sécurité, ont ainsi été proposées. Parmi les méthodes ainsi définies, certaines posent la question de la réutilisation de connaissances capitalisées afin de faciliter l'élucidation et d'améliorer la complétude des exigences [1]. Nous avons développé au cours de travaux précédents une méthode qui s'appuie sur des ontologies pour guider la découverte des besoins [2]. Les ontologies sont connues pour être des sources riches de connaissances et, étant structurées et dotées de mécanismes de raisonnement, elles forment un outil puissant pour guider l'analyse des exigences [3]. Nos expériences nous ont cependant montré qu'il était particulièrement crucial de bien choisir ces ontologies afin de maximiser les chances de produire des résultats utiles,
En effet, Les experts impliqués dans l'évaluation [2] ont révélé que étant générique, les menaces dans l'ontologie utilisée ne produisent pas des exigences spécifique au domaine bancaire (l'étude de cas était dans le domaine bancaire).
Nous proposons dans ce projet de recherche, de mobiliser deux types d'ontologies pour supporter le processus d'ingénierie des exigences de sécurité : les ontologies de sécurité, et les ontologies de domaine. L'hypothèse principale que nous souhaitons démontrer est que le recours combiné à ces deux types d'ontologies pour guider l'élucidation des exigences est plus efficace que lorsqu'on ne se base que sur des ontologies généralistes. Notre démarche de recherche s'appui sur la méthodologie de recherche design science [4]: après avoir mené une recherche bibliographique et des études empiriques (études de cas, interviews d'experts) pour bien formuler notre question de recherche et nos hypothèses, nous avons élaboré une méthode à base de règles capables de proposer de nouveaux éléments à ajouter à une spécification d'exigences de sécurité. La troisième étape de notre projet visera à valider notre méthode de manière empirique, afin d'en démontrer l'effectivité et la scalabilité.

[1] M. Saeki, « Semantic Requirements Engineering », in *Intentional Perspectives on Information Systems Engineering*, S. Nurcan, C. Salinesi, C. Souveyet, et J. Ralyté, Éd. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, p. 67‑82.
[2] C. Salinesi, E. Ivankina, et W. Angole, « Using the RITA Threats Ontology to Guide Requirements Elicitation: an Empirical Experiment in the Banking Sector », in *First International Workshop on Managing Requirements Knowledge, 2008. MARK '08*, 2008, p. 11 ‑15.
[3] V. Castañeda, L. Ballejos, M. L. Caliusco, et M. R. Galli, « The Use of Ontologies in Requirements Engineering », *Global Journal of Research Engineering*, vol. 10, nº 6, nov. 2010.
[4] A. Hevner et S. Chatterjee, *Design Research in Information Systems: Theory and Practice*, 1re éd. Springer, 2010.

Doctorant (email) : Amina Souag (Amina.Souag@malix.univ-paris1.fr)
Directeurs de Thèse : Pr. Camille Salinesi & Pr. Isabelle Wattiau
Laboratoire, Université : Centre de Recherche en Informatique (CRI), Equipe ISID (CNAM)

A structured approach for security requirements definition based on security and domain ontologies

Keywords: security requirements, ontologies, security, elicitation, analysis.

Abstract:

In recent years, the issue of information system security (confidentiality, availability, integrity, traçability) has become a major concern which must be taken into account early in the development cycle of systems, especially in the phase of requirements engineering (RE).

Several studies have been conducted on security requirements engineering. Different useful approaches have been proposed for defining security requirements. Several methods raise the question of reusing capitalized knowledge to facilitate the elicitation and improve the completeness of requirements[1]. In previous work we developed a method that relies on ontologies to guide the discovery of requirements [2]. Ontologies are known to be rich sources of knowledge, and, being structured and equipped with tools of reasoning, they form a powerful tool to guide requirements analysis [3]. Our experience has shown that it is particularly important to choose well the ontologies used in order to maximize the chances of producing useful results. In fact, experts involved in the evaluation [2] complained that being generic, threats in the ontology used do not produce specific banking security requirements (case study was in banking sector). We propose in this research project to mobilize two types of ontologies in the process of requirements engineering: security ontologies, and domain ontologies. The main hypothesis we want to demonstrate is that the combined use of these two types of ontologies to guide the discovery of requirements is more effective than relying on general ontologies. Our research methodology is adapted from [4]: after conducting a literature review and empirical studies to fully formulate our research question and hypotheses, we developed a method based on rules which can introduce new elements to add to a specification of security requirements. The third step in our project will validate our method empirically to demonstrate the effectiveness and scalability.

[1] M. Saeki, « Semantic Requirements Engineering », in *Intentional Perspectives on Information Systems Engineering*, S. Nurcan, C. Salinesi, C. Souveyet, et J. Ralyté, Éd. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, p. 67‑82.

[2] C. Salinesi, E. Ivankina, et W. Angole, « Using the RITA Threats Ontology to Guide Requirements Elicitation: an Empirical Experiment in the Banking Sector », in *First International Workshop on Managing Requirements Knowledge, 2008. MARK '08*, 2008, p. 11 ‑15.

[3] V. Castañeda, L. Ballejos, M. L. Caliusco, et M. R. Galli, « The Use of Ontologies in Requirements Engineering », *Global Journal of Research Engineering*, vol. 10, nº 6, nov. 2010.

[4] A. Hevner et S. Chatterjee, *Design Research in Information Systems: Theory and Practice*, 1re éd. Springer, 2010.