Mereotopological Analysis of Formal Concepts in Security Ontologies

Gonzalo A. Aranda-Corral and Joaquín Borrego-Díaz

Abstract. In this paper an analysis of security ontologies, using an mereotopological interpretation of the relationship amongst their classes, based on the entailment in the ontology, is presented. The analysis is carried out by means of a graphical tool (called Paella) that implements such an interpretation and it can suggest the potential debugging of anomalies. The analysis also suggests how to interpret the representational anomalies.

1 Introduction

The envisioned Semantic Web (SW) aims to turn the information of the current web into knowledge for solving the informational chaos inherent with the current WWW, by providing trustworthy processing of the information. Its progressive introduction -mostly by institutions and companies- will represent a fundamental change in the understanding of information on the Internet, and, more importantly, it will change the management of digital information about consumers, governments, users, etc. Nevertheless, from the social and security point of view, certain risks exist with these improvements. One of these is the globalization of digital information, which was not considered at the beginning of the current WWW. Another risk could be the deficient transformation/management of the information. In the case of Semantic Web, it presents the opportunity to evaluate and reflect upon them, from different perspectives: computational, epistemological, logical, trustworthy, etc.
Ontologies are formal theories of Knowledge that bridge different resources, solving the interoperability problem at a formal level in SW. Therefore, Knowledge processing needs of a sound understanding of ontologies. However, then formal languages proposed for the representation of ontologies can not be used by non-experts in ontologies, for example, experts in information security. Thus evaluation process is a key stage in Knowledge Engineering (KE) applied to security. In fact, The introduction of SW technologies can produce a ”semantic divide” which can not be avoided by implementing standard technologies. There are some formal semantic literacy tasks, which are necessary to produce technologies that make the formal aspects invisible to the user. Other cases where the problem appears are where the SW is applied in Web 2.0 and Open Data Strategies (ODS). The use of SW techniques within the Web 2.0, needs paradigms where ontologies are transparent (i.e., Freebase\[^1\] or OpenCalais service\[^2\]) as well as tools to represent the ontology in a user friendly way. This would be beneficial to users who attempt to understand the knowledge that companies or institutions hold about them, and how it is interpreted. Likewise, the adoption of Web 2.0 strategies in institutions and companies also need such technologies. A closely related issue which has recently emerged is the adoption of Open Data Strategies (ODS) by institutions. ODS causes citizens to be interested in the data stored about them. ODS combined with SW tools can provide a best representation of the data through interoperability. Therefore, we can think about this and we can understand how we are viewed as a consumer/user. An image that emerges from the knowledge that companies possess about us, through personal data and the ontology used. Misinterpretation of information (by the user or the system) is an evident danger.

The aim of this paper is to show how to analyse the robustness of security ontologies using automated and visual reasoning -implemented in a semantic tool- as well as to detect some kind of representational anomalies. From this analysis, we try to enhance the conceptual information processing of security ontologies by means of a Semantic Information Representation tool. The tool lets non expert users -on ontological engineering- both to understand and to debug the relationships among critical security concepts in a logical and trustworthy method.

The structure of the paper is as follows. The next section considers the role of ontological engineering issues in security ontologies. In Sect. 3 we present the formal principles of ontology visualization based on reasoning services that represent the logical basis of the Paella tool, described in Sect. 4. Sect. 5 is devoted to discussing the main results of the analysis of a set of security ontologies. The paper ends with some remarks on future work.

2 Knowledge Representation in Security Ontologies

The ontology-based approach enables the definition of the security concepts and their dependencies in a comprensible way both for humans, and software agents\[^1\].

\[^1\] www.freebase.com
\[^2\] http://www.opencalais.com