SecAOnto: A Conceptual Model of Security Assessment

Ferrucio de Franco Rosa, CTI, Brazil & UNIFACCAMP, Brazil
Luiz Antonio Lima Teixeira Junior, CTI, Brazil
Rodrigo Bonacin, CTI, Brazil & UNIFACCAMP, Brazil
Mario Jino, FEEC, University of Campinas, Brazil

ABSTRACT

Security assessment is crucial to the implementation and use of secure web portals. Literature reports studies about knowledge representation models for systems assessment and information security areas; however, there is a lack of conceptual formalization for the security assessment area. The security assessment ontology (SecAOnto) objective is to formalize knowledge on security assessment. It is based on ontologies, taxonomies, vocabularies, glossaries, and market guidelines. This paper presents an application of SecAOnto with the objective of identifying concepts in descriptions of security assessment items; the coverage of security characteristics is determined by using a coverage calculus algorithm. The application of SecAOnto and of the coverage calculus algorithms to the well-known standard ISO/IEC 27001 highlights its expressiveness. The proposal is useful for security experts and researchers in the context of security assessment, as well as to support web-based conceptual architectures.

KEYWORDS


INTRODUCTION

Web portals are important components in the context of the Internet; for example, cloud computing is a means of delivering Information Technology business services (Alhawari, Jarrah, & Hadi, 2017). Security, privacy and trust are key aspects of the new Web portals and mobile applications. Various applications (e.g., e-Wallets (Gandon & Sadeh, 2004)) access personal resources, among other critical information, increasing the need for secure and trusted interoperable systems. Trust is core issue of human interaction with Web portals, once it is necessary for users to act under uncertainty and in risk situations (Artz & Gil, 2007).

Development, maintenance and assessment of secure and trusted interoperable Web systems, and fault tolerant web systems (Nascimento, Rubira, Burrows, Castor, & Brito, 2014), demand a rigorous conceptual support. Literature presents advances in frameworks for the security assessment process (e.g., (ISO/IEC, 2013)), nevertheless formally described models, such as ontologies are still needed (Rosa & Jino, 2017).

Theoretical knowledge regarding information security assessment should be better systematized and organized. Frequently information systems are evaluated based on experts’ previous experience.
In this context, the security assessment can be enhanced by the formal conceptualization of the domain (Rosa, Jino, & Bonacin, 2017). The semantic web ontologies may provide means to formally represent the security assessment domain in a machine and human interpretable format (Feledi & Fenz, 2012). We propose to use ontologies for representing and structuring the knowledge of the security assessment domain.

Various efforts have investigated alternatives and proposed ontologies with the objective of representing the Information Security domain and subdomains. Although there are studies relating software development processes, as a whole, with information security ontologies (e.g., (Kang & Liang, 2013; Mouratidis & Giorgini, 2008; Wen & Katt, 2018)), there is still a need for ontologies representing the relationship between the fields of “Information Security” and “Software Assessment” in a comprehensive and deeply way. The investigation of vulnerability as well as attacks is the basis for various of security assessment methods. This approach does not consider rigorous assessment coverage criteria (Rosa, Bonacin, Bueno, & Jino, 2018). The establishment of relations between concepts of “Information Security” and “Software Assessment” are necessary to determine these criteria. This may make explicit the coverage of assessed security characteristics, for instance, by its measurement; a minimal percentage of assessment coverage could be required, going beyond defense-attack issues and coverage of known vulnerabilities, providing a higher level of resilience.

Our objective is to use an ontology to represent the concepts of the Security Assessment area. The Security Assessment Ontology (SecAOnto) aims to formally represent the particularities of this area.

The ontology engineering process starts by analyzing the existing works on Information Security and Systems Assessment areas. The engineering approach is based on Barbosa, Nakagawa, & Maldonado (2006), Bermejo (2007), and Obrst, Chase, & Markeloff (2012), following the Guarino’s ontology classification (Guarino, 1998); we propose: (1) the Information Security models is reused as domain ontology; (2) the System Assessment models is reused as task ontology; and (3) the SecAOnto is developed an application ontology, representing concepts from both contexts.

We proposed a coverage calculus algorithm to support the validation of the SecAOnto. This algorithm uses the ontology to identify assessment items. Using the Jena Framework (The Apache Software Foundation, 2017), we search which concepts are represented in a Knowledge Source (KS), and then we assign Assessment Dimensions (DM) and Security Properties (PP). The coverage of security assessment characteristics is calculated by means of distances calculated using the ontology; this is an important step for the generation of security assessment criteria.

The construction of the SecAOnto comprises an effort of several years, including a systematic review of the literature (Rosa & Jino, 2017; Rosa, Jino, & Bonacin, 2017) and the conception of a first version, which contained only the core of the ontology (Rosa, Bonacin, et al., 2018). This paper advances by presenting an extensive model of SecAOnto version 4 (March 2019), as well as its application in a study. Discussion from our experience with the engineering process and the application of the ontology in coverage calculus is also presented. Thus, our main contributions are two-fold:

- The SecAOnto version 4, which formalize concepts of Security Assessment field, linking them to Information Security and System Assessment concepts;

The remaining of paper is organized as follows: the second section summarize literature review on security assessment modeling; the third section describes SecAOnto including its main concepts and relationships aiming at providing a formal model for security assessment field, i.e., it provides
State Portals as a Framework to Standardize E-Government Services
www.igi-global.com/chapter/state-portals-framework-standardize-government/17994?camid=4v1a