Ontology-based Framework for Information Security Risk Management

**Name des Kandidaten:** Andreas Ekelhart  
**Name der Begutachter:**  
O. Univ. Prof. Dr. A Min Tjoa (Technische Universität Wien)  
Prof. Dr. Günther Pernul (Universität Regensburg)

**Abstract:**  
The ever-growing dependence on information technology leads to an increase in expensive information security incidents and failures. While researchers have proposed several approaches to managing information security risks, several shortcomings of existing approaches can still be identified. Complex relationships in the information security domain, error-prone manual application of the information security knowledge to the organizational infrastructure, subjective impact value determination, and incomplete knowledge during the control evaluation can lead to an inadequate information security strategy and, therefore, pose a risk to the organization's mission.

As a first step in addressing these shortcomings, this thesis elaborates on the development of a formal knowledge model (security ontology), comprising relevant security concepts, which can be applied by organizations to model their own environment and subsequently retrieve answers to security-relevant questions. Analysis of existing work in security ontologies forms the basis for the developed security ontology, and the model is evaluated by means of competency questions. Thereafter, we will show how the security ontology can be extended to include advisory knowledge. On this basis, an architecture for a semantic Computer Security Incident Response Team is presented. To support users in the information security risk management (ISRM) process, a framework for automated ISRM is presented, which covers all ISRM phases outlined by major ISRM methodologies. Again, this approach builds on the formal security knowledge model. In addition, extensions for each phase, such as risk determination and control identification, are introduced. While all phases are covered, special focus is placed on a novel technique to determine importance values of assets, based on business process analysis. To demonstrate how this ISRM framework can be applied in real life, a prototype was developed and an example case was carried out. Results showed the benefits of the framework, e.g., that security knowledge is provided in a consistent and comprehensive way, consistent risk values can be automatically calculated, and users are supported in the selection of efficient controls.

Most ISRM-related research aims to improve ISRM, but there is still a considerable lack of thorough verification, validation and evaluation of the developed approaches and their implementation. Focusing on the problem of sound verification, validation and evaluation of ISRM, the results of an ISRM literature research are presented to provide an overview of applied verification, validation and evaluation methods. Then, I will discuss in which ISRM phases the methods should be applied. This research provides a reference for researchers and users of ISRM approaches who aim to establish trust in their results, and draws conclusions on the current status of ISRM verification, validation and evaluation.