Abstract

Data and service security is essential in any information system. New threats and attacking methods arise day by day. Analysis of existing practices and design of new defense methods is important. Instead of real systems, often their models are used in this process. This thesis introduces ontologies as models for data and service security analysis and design. Ontologies are powerful tools because of their expressing strength. Their power is based on the fact that conclusions derived from them via reasoners (inference engines) are logically correct. On the design side, once the ontology model of the system and its inputs are available, certain properties of the output can be calculated. On the analysis side, given the system and the output, some properties of the input can be deduced. On the modeling side, observed (real) outputs for given inputs may be used to refine the model. Furthermore, internal workings of the model of the system reveal effect/error propagation paths. This, along with the output, provides important information on the expectable effects of various inputs.

This thesis presents ontology-based solutions, for rating IT systems based on their models, from security point of view. Rating is achieved by reasoning software. Based on these ratings a numerical computation of the effects and costs is performed. This computation is solved by conventional programming methods as the ontology and the reasoner have limited arithmetic capability.