Title: Risk Management for Usage Control in Services

Abstract

Modern computer systems like Grid, Web services, Cloud are distributed and highly dynamic by their nature. The systems change frequently, and the changes impact different qualities of the system including security. The risk assessment could be used to capture the general state of the security level of the systems. However current risk assessment is a long-lasting and tedious procedure and, as a result, is not very suitable for the evaluation of dynamic and distributed systems. We propose a new framework for rapid assessment of changing risk observing mutable security parameters of the system.

The risk measures the influence of the uncertainties about parameters presented in the system. There are two types of uncertainties: unintentional and intentional. Unintentional uncertainties are caused by the natural peculiarities of the system. Intentional ones are connected with deliberate actions performed by the attacker trying compromise the system.

We provide an approach for the evaluation of unintentional risks connected with freshness of parameters. The approach is used to enhance the usage control model. The usage control (UCON) model demands for continuous control over objects of a dynamic system (e.g., Grid or Service-oriented architecture). Access decisions are done several times within a usage session and are performed on the basis of mutable attributes. Values of attributes available for decision making process sometimes are not up-to-date in modern highly dynamic and distributed systems, because attributes may be updated by several entities and reside outside the system domain. Thus, the access decisions about a usage session are made under uncertainties, while existing usage control approaches are based on the assumption that all attributes are up-to-date. Our approach helps to make a rational access decision even if some uncertainty presents. The approach uses the Markov chains (discrete-time or continuous-time) in order to compute the probability of unnoticed changes of attributes and risk analysis for making a decision. The approach can be adopted for evaluation of several types of intentional risks.

However, in general the assessment of intentional risks requires another model to be used. We developed formal models for intentional risk and security metrics. Security metrics are the tools for providing correct and up-to-date information about a state of security parameters. The models helped us to discover how changes of security metrics impact on the risk. We showed that all metrics play only a small role when the overall risk is computed.

The model for intentional risk allowed us to propose a risk assessment approach for Service-oriented Architecture. In Service-oriented Architecture data belonging to a client (data provider) is often processed by a service provider (data consumer). During this processing the data can be compromised. A client wants to be sure that its data is used in the least risky way while is under provider's control. Both the client and the provider have their own security preferences, which can be seen as constrains for the security parameters (attributes). The client can assess the risk of data processing by the provider analyzing constrains. The risk level should be low when access to the data is granted and should remain low during the whole interaction and, maybe, some time after. Therefore, a client has to consider closely various providers and decide which one provides the service with the smallest risk. More importantly, the risk has to be constantly recomputed after granting the access to the data, i.e., usage of data must be controlled. We show how to select a service provider using risk, re-evaluate the risk level when some changes have happened and how to improve an infrastructure in order to reduce the risk level. Our current step is to extend this line of research for such new dynamic system as Cloud.