Security Assurance Assessment for Multi-layered and Multi-tenant Hybrid Clouds

PhD THESIS by: mag.ing.el.techn.inf. Aleksandar Hudic

Registration Number: 1029196

Supervisor: Dr. techn. Edgar R. Weippl

Reviewers:

Assistant Professor Stjepan Gros University of Zagreb,
University Professor Rene Mayrhofer Johannes Kepler University Linz

ABSTRACT:

This thesis is based on five publications related to the area of security assurance for hybrid clouds which were published at conferences or in journals by IEEE and Elsevier. Cloud computing is an ongoing research field that received an increasing attention in last several years, as new challenges arise in the cloud ecosystem on daily basis especially with the new hybrid cloud models coming to the scene. Meanwhile, the old challenges with regards to security, privacy and especially transparency haven’t been comprehended or addressed properly to keep up with the technological momentum caused by the cloud paradigm. Sharing security sensitive information in a cloud environments has become a main obstacle due to the immense lack of transparency. Hence, this thesis addresses this challenges, in particular, transparency of cloud providers that for the given security objectives there are supporting measures in place. The thesis is especially concerned with the security and transparency with regards to security critical services especially with regards to hosting them in hybrid multi-layered and multi-tenant environments.

To comprehend the complexity of hybrid cloud environments that can be composed of multiple layers and owned by multiple stakeholder we illustrate a composite multi-layer reference architecture model. The main objective of this model is to observe multidimensional critical infrastructure systems at individual levels from different viewpoints, namely those of multi-provider and multi-tenant, and different stakeholders. Furthermore, we analyze the challenges, objectives and requirements for deploying critical infrastructure services to cloud environments with regards to transparency and security. The challenges that we identified highlight the shortcoming of cloud providers to support transparency especially with regards to the hybrid cloud solutions. To overcome this gap this thesis propose a novel model for holistic security assurance assessment that addresses the interdependencies between both individual components and abstraction levels in hybrid cloud environments. The approach offers the ability to address each individual component of a cloud based infrastructure, regardless if it is a physical server, virtual container, or a high level service, in a structural manner by including all its interdependencies. The flexibility of the approach lies in the composite structural design of the security assurance assessment framework that adheres the Common Criteria and enhances it to achieve higher level of granularity when assessing services. Most importantly, unlike standard approaches for security assessment like certification or auditing our model offers continuous security assessment ability of hybrid cloud environments where we can have competitive cloud provider that deliver one single
service. Lastly, our security assurance assessment model prevents the exposure of internal security sensitive information of a cloud provider via its novel security assurance assessment model that operates on abstracted security information sets. Furthermore, we propose a comprehensive life-cycle for designing, developing and deploying secure cloud services in line with standards, regulative compliance, and best practices. In addition, the proposed life-cycle integrates iterative security requirements engineering from high level objectives to security properties used for security validation entities through both development and production phase of cloud services. The life-cycle aligns and integrates the security assurance assessment model, by at the same time supporting it with security requirements, in the final production phase to enhance transparency.