Chapter 41
A Structured Method for Security Requirements Elicitation concerning the Cloud Computing Domain

Kristian Beckers
Univeristy of Duisburg-Essen, Germany

Ludger Goeke
ITESYS Institute for Technical Systems GmbH, Germany

Isabelle Côté
ITESYS Institute for Technical Systems GmbH, Germany

Selim Güler
EASY SOFTWARE AG, Germany

Maritta Heisel
University of Duisburg-Essen, Germany

ABSTRACT

Cloud computing systems offer an attractive alternative to traditional IT-systems, because of economic benefits that arise from the cloud's scalable and flexible IT-resources. The benefits are of particular interest for SME's. The reason is that using Cloud Resources allows an SME to focus on its core business rather than on IT-resources. However, numerous concerns about the security of cloud computing services exist. Potential cloud customers have to be confident that the cloud services they acquire are secure for them to use. Therefore, they have to have a clear set of security requirements covering their security needs. Eliciting these requirements is a difficult task, because of the amount of stakeholders and technical components to consider in a cloud environment. Therefore, the authors propose a structured, pattern-based method supporting eliciting security requirements and selecting security measures. The method guides potential cloud customers to model the application of their business case in a cloud computing context using a pattern-based approach. Thus, a potential cloud customer can instantiate our so-called Cloud System Analysis Pattern. Then, the information of the instantiated pattern can be used to fill-out our textual security requirements patterns and individual defined security requirement patterns, as well. The presented method is tool-supported. Our tool supports the instantiation of the cloud system analysis pattern and automatically transfers the information from the instance to the security requirements patterns. In addition, they have validation conditions that check e.g., if a security requirement refers to at least one element in the cloud. The authors illustrate their method using an online-banking system as running example.

DOI: 10.4018/978-1-4666-8111-8.ch041

1. INTRODUCTION

It is hard to find the *right* cloud computing offer with regard to security, when one does not know what *right* is. The definition of precise security requirements provides the means define this right with regard to cloud security. After identifying the cloud security needs, one has to select security measures that fulfill the requirements. We provide a structured method to address this problem, so that SME's can use it with little effort. We base the method on known security guidelines and standards like ISO 27001 to ensure a state-of-the-art approach.

The term *cloud computing* describes a technology as well as a business model (Armbrust et al., 2009). According to the *National Institute of Standards and Technology (NIST)*, cloud computing systems can be defined by the following properties (Mell & Grance, 2011): the cloud customer can require resources of the cloud provider over *broad network access* and *on-demand* and pays only for the used capabilities. Resources, i.e., storage, processing, memory, network bandwidth, and virtual machines, are combined into a so-called *pool*. Using cloud computing services is thus an economic way of acquiring IT-resources. The dynamic acquisition and scalability, yet paying only what was used, makes cloud computing an interesting alternative for a large amount of potential customers. The pay-per-use model includes guarantees such as availability or security for resources via customized *Service Level Agreements (SLA)* (Vaquero et al., 2008). However, the customers are also hesitant to sign up with a cloud provider. In 2009, the International Data Corporation[1] conducted a survey to find out why customers are so hesitant. The survey showed that the lack of trust in cloud security measures is at the top of the list why people avoid using cloud services. The customers fear that managing and storing critical data and executing sensitive IT-processes beyond their grasp has an impact on the security of their data and IT-processes, respectively.

To (re-)gain this trust some well-known cloud providers have started to certify their cloud computing systems according to the ISO 27001 standard to show potential customers that they take their concerns, e.g, considering security, seriously. Unfortunately, it is not always clear to customers what their security requirements actually are.

Our approach aims at helping potential cloud customers to elicit their security requirements. We provide patterns that result in a set of security requirements once they have been instantiated. The patterns are embedded in a method that guides a potential cloud customer through the elicitation process in a structured manner. The method uses an enhanced version of the *Cloud System Analysis Pattern* (CSAP) introduced in Beckers et al. (2011). It is possible to add security requirements patterns, if the patterns from existing patterns do not suffice. Our method proposes to use the instantiated requirements patterns to select security measures. We integrate published best practices in our method, e.g., from the BSI recommendations (2012). In addition, we recommend to use existing catalogues of security controls in this part of the method, e.g., from the ISO 27001 standard (2005).

We contribute a meta-model that specifies the structure of the CSAP. The meta-model enables us to specify validation conditions to check, e.g., the consistency of the security requirements amongst each other. In addition, we provide tool support for instantiating the cloud system analysis pattern as well as an automatic transfer from the information of the instance to the security requirements patterns.

We use an online-banking system as running example to show the applicability of our approach.

The paper is structured as follows: In Sect. II, we briefly introduce the case study serving as a running example throughout the remainder of this paper. With Sect. III, we portray our approach. Section IV provides an overview of the technical realization of our current tool support. In Sect. V, we evaluate and discuss our approach. We conclude the paper with Sects. VI stating related work and VII summarizing our work and giving directions for future research.