Chapter 40
Threatening the Cloud:
Securing Services and Data by Continuous, Model-Driven Negative Security Testing

Philipp Zech
University of Innsbruck, Austria

Michael Felderer
University of Innsbruck, Austria

Philipp Kalb
University of Innsbruck, Austria

Ruth Breu
University of Innsbruck, Austria

ABSTRACT

Today's increasing trend towards outsourcing IT landscapes and business processes into the Cloud is a double-edged sword. On the one side, companies can save time and money; however, on the other side, moving possible sensitive data and business processes into the Cloud demands for a high degree of information security. In the course of this chapter, the authors give an overview of a Cloud's various vulnerabilities, how to address them properly, and last but not least, a model-driven approach to evaluate the state of security of a Cloud environment by means of negative testing. Besides, the authors incorporate the idea of living models to allow tracking and incorporating of changes in the Cloud environment and react properly and, more important, in time on evolving security requirements throughout the complete Cloud Life Cycle.

INTRODUCTION

Since the early beginnings of software development, testing has always been an important part of assuring the proper and required behavior of a system. However, still nowadays testing is often the one phase during the Software Development Lifecycle (SDLC) which is mostly performed very poorly and by far does not cover the complete software product by incorporating all its requirements, especially when it comes to security testing of a software system. This is mainly motivated by the fact, that often only positive requirements are used, yet the idea of incorporating negative requirements, describing a successful abuse of the system, is neglected. However, the usage of such negative requirements should be motivated strongly, as besides the positive requirements,

DOI: 10.4018/978-1-4666-8473-7.ch040

negative requirements also describe part of the possible behavior of a system, which demands to be examined with the intention to detect and mitigate it.

Considering today's advancements in the area of software development, it is quite obvious that software security has to be ascribed an important status. This is mainly motivated by the growing complexity and usage of software systems in high security sensitive domains, i.e., eHealth. Talking about contemporary advancements in software development, especially one paradigm of salient relevance protrudes, namely Cloud Computing. Being mostly used as a buzzword in the early 2000s, Cloud Computing nowadays has grown to a quite mature technology that has gained lots of acceptance, especially in the corporate IT world. This growing acceptance mainly is because of a Cloud's great opportunities in the area of IT outsourcing, allowing small and mid-sized business to save vast amounts of time and money. The key factor for this success of outsourcing lies in a cloud's elasticity. This concept of dynamically distributing resources through virtualization and intelligent hardware management allows companies to successfully move complete IT landscapes and business processes into the Cloud, by in the end only being accounted for the computing time they actually consumed, thereby eradicating wasted idle times.

However, as it is quite often with newly approaching technologies and computing paradigms, despite its opportunities, a Cloud also has to deal with various drawbacks in terms of information security. Despite the classical vulnerabilities, inherent in the employed technologies, a Cloud introduces various security risks, specifically inherent in the idea of Cloud computing (Siemens, 2010) (CloudSecurityAlliance, 2011). One of the major security concerns coming along with the idea of Cloud Computing is data protection. Inside a Cloud loads of users are doing their computations side by side, often using sensitive data. Hence, a Cloud has to assure that user data is protected vigorously to avoid accidental or malicious leakage. Another important issue, besides proper data protection, is the possible risk of a Cloud environment to degenerate into a hacker's playground. Compromising such an environment with all its computational resources and power allows a hacker to launch rogue attacks against institutions of any kind. Yet, this by far is not the complete story of a vulnerable Cloud, there are a lot of other considerations to be taken into account, i.e., protecting running applications and prevent loss of reputation or financial resources, yet it already indicates the relevance of proper security assurance. Additionally, by considering the security of a Cloud, one has to think differently as opposed to a stand-alone application. In contradiction to the classical SDLC the actual lifecycle of a Cloud differs seriously. Whereas in the classical SDLC security is mainly examined during the testing phase, in the Cloud Lifecycle (CLC), security is an evolving requirement, which needs to be taken into account throughout the whole uptime of the Cloud. Changing or new deployments of applications, newly virtualized instances of different platforms, all these alterations actually change the current configuration of the Cloud and demand for reevaluating the security of the Cloud environment, as the performed changes often introduce new flaws.

Based on the above observations, we introduce a novel, two-tracked model-driven approach for the risk-based security testing of Cloud systems to improve Cloud environment security. On the one side, to examine the service interface, put another way, the attack surface of a Cloud, a risk analysis is performed on the system model of the Cloud Under Test (CUT). This risk analysis yields a tailored risk model, used to generate a dedicated misuse case model, describing possible malicious activities to abuse the Cloud. Subsequently, this misuse case model is used to generate executable test cases by employing an own code generator. On the other side, to assure proper data protection in the Cloud, we employ XACML (OASIS,