Chapter 45
Security Risks in Cloud Computing:
An Analysis of the Main Vulnerabilities

Belén Cruz Zapata
University of Murcia, Spain

José Luis Fernández Alemán
University of Murcia, Spain

ABSTRACT

Any software system is exposed to potential attack. The recent and continuous appearance of vulnerabilities in software systems makes security a vital issue if these systems are to succeed. The detection of potential vulnerabilities thus signifies that a set of policies can be established to minimize their impact. This therefore implies identifying the risks and data to be protected, and the design of an action plan with which to manage incidents and recovery. The purpose of this chapter is to provide an analysis of the most common vulnerabilities in recent years, focusing on those vulnerabilities which are specific to cloud computing. These specific vulnerabilities need to be identified in order to avoid them by providing prevention mechanisms, and the following questions have therefore been posed: What kinds of vulnerabilities are increasing? Has any kind of vulnerability been reduced in recent years? What is the evolution of their severity?

INTRODUCTION

Many cloud applications are currently widely and successfully used (i.e. Google App Engine, Amazon's Computer Cloud Amazon Web Service and Microsoft Azure Service Platform). Although cloud computing is a growing technology, no key player leads this revolution. The cloud saves money and has the backing of many large software vendors (Lillard, Garrison, Schiller, & Steele, 2010). However, one of the main reasons for the slowing down in the growth of cloud computing is that of security (Subashini & Kavitha, 2011). A few examples of this are two real incidents which occurred in 2009. One of them is Salesforce.com which suffered an outage that locked more than

DOI: 10.4018/978-1-4666-4301-7.ch045

900,000 subscribers out of crucial cloud computing applications and data needed to transact business with customers (Ferguson, 2009). Another example is the smart phone known as "Sidekick" with which users (over 800,000) temporarily lost personal data which was accessed as a cloud service. The outage lasted almost two weeks, and some losses might have been permanent (Cellan-Jones, 2009).

Data protection and data privacy are extremely important, and in a cloud computing infrastructure the detection of potential vulnerabilities is therefore of paramount importance. A cloud computing model may have the same kind of vulnerabilities that are detected in conventional computing models, while other vulnerabilities are intrinsic to the technology used by cloud computing. From a cloud customer perspective, the consequences and ultimate cost of a security attack is exactly the same, regardless of whether it has occurred within a cloud or a conventional IT infrastructure. For a cloud service provider, however, the perspective is somewhat different. If a vulnerability is prevalent in state-of-the-art cloud offerings, then it must be regarded as cloud-specific.

Being aware of these vulnerabilities is the best mechanism for prevention. The Law of Vulnerabilities 2.0 (Wolfgang Kandek, CTO & Qualys, Inc., 2009) states that "80% of vulnerability exploits are now available within single digit days after the vulnerability's public release". The cloud provider is responsible for providing secure cloud instances, which should ensure users privacy, maintain data integrity and guarantee that information and information processing is available to clients upon demand. It is therefore important to identify those vulnerabilities that are specific to cloud computing. Since risks cannot be completely eliminated, they need to be lowered to acceptable levels.

In order to better understand the singularities of cloud computing vulnerabilities, a set of essential characteristics should be considered:

- **On-demand self-service:** A user can provide services automatically without requiring human interaction with the service provider.
- **Broad network access:** Services are available via the network through standard mechanisms.
- **Resource pooling:** Resources are pooled to serve multiple consumers, and are dynamically assigned and reassigned according to consumer demand.
- **Rapid elasticity:** Resources can be rapidly and elastically provided in order to quickly scale out and scale in.
- **Measured Service:** Resource usage can be monitored, controlled, and reported.

If a clear idea of concepts such as vulnerability, threat or risk is to be obtained, then it is first necessary to describe these terms. A threat is a potential cause of an unwanted impact on a system or organization (ISO 13335-1). Threats fall into two categories, known as vulnerabilities and exposures. According to MITRE's CVE Terminology (MITRE, 2011), vulnerability is a mistake in software that can be directly used by a hacker to gain access to a system or network. It is therefore a state in a computing system (or set of systems) which:

- Allows an attacker to execute commands as another user;
- Allows an attacker to access data that is contrary to the specified access restrictions for that data;
- Allows an attacker to pose as another entity; and
- Allows an attacker to conduct a denial of service.

An exposure, meanwhile, is defined by MITRE's CVE Terminology as a system configuration issue or a mistake in software that allows