Chapter 9
The Security of Cloud Infrastructure

Massimo Civilini
Cisco Systems® Inc., USA

ABSTRACT
The development of commercial Cloud environments has been fueled by the introduction of new technologies which have changed the interactions between the base components of a legacy IT infrastructure: computing, networking, and storage. In particular, the security of data and operations has been impacted by these changes, making the legacy security infrastructure no longer adequate to support new scenarios. This chapter illustrates how base infrastructure operations like software provisioning and resource virtualization are critical from a security viewpoint. It will also discuss the mitigation solutions available in guaranteeing an adequate level of security in the Cloud.

INTRODUCTION
The Cloud environments available today allow single home users to access extended computing and storage services as well as enterprises that outsource part of their data centers. This permits users to pay only for the resources they utilize, avoiding onerous investments in hardware, software, physical spaces, and maintenance. The Cloud concept is also appealing on a smaller scale. Because of the advantages offered by an elastic Cloud, many companies are implementing infrastructures that mimic the general Cloud concept but are personalized to their private infrastructure and needs, realizing a Cloud environment which is smaller in size, closed and private. These types of Cloud are important from a development and application viewpoint because they are extensible and allow a practical approach that is focused on customer needs, business analysis, technical solutions and marketing opportunities.

DOI: 10.4018/978-1-4666-1631-8.ch009
However, these new capabilities, when connected with the Cloud concept, come at a price; the resulting environments are extremely challenging to manage from a security standpoint. The difficulty arises from the combination of the need for open network architecture and distributed resource management, thereby crossing the normal client-server security infrastructure which is at the base of everyday network security concepts.

The Cloud architecture is changing the basic interactions between the components of infrastructure and a new approach must be devised to guarantee security. Firewall, SSL and NAT are still necessary but are no longer sufficient to protect data in the Cloud. These general concerns regarding the Cloud are shared between all the different types of Cloud architectures and have an impact on the Cloud services at every level.

The Cloud infrastructure is the lowest level of deployment; Cloud services are built on top of it. A security flaw at this level has an immediate negative impact on the services. This is also the place where platforms integrate where convergence is discussed in standard committees and where commercial reasons drive the steps forward, with the result that, sometimes, the best solutions are sacrificed in favor of compatibility or revenues. These reasons explain why we still have, for example, a thirty year old BIOS infrastructure in the latest and most powerful server in the Cloud or limitations in the migration of virtual machines.

The chapter will illustrate the critical security points for a Cloud infrastructure by describing two of the main operations at infrastructure level: the provisioning of software and the virtualization of resources. These operations are at the core of the Cloud infrastructure and contain the basic problems seen on the low level side and high level side, represented by platform and applications. Provisioning deals not just with the infrastructure itself, but it regulates the possibility to offer Platform services and Software services, delivering application and VM software. In that section the problems at the base of the Cloud deployment and security architecture are introduced: hardware identity, VM identity, virus protection, and cloud dynamics. The problems of integration among platforms and among different Cloud infrastructures are presented in the resource management section and hybrid Cloud section respectively.

BACKGROUND

The development of a fast, cost-effective network infrastructure and the availability of high performance computational and storage platforms fueled the creation of Data Centers as aggregation points for the IT infrastructure. The Cloud computing concept, favored by the heavy adoption of technologies like virtualization and self-management, has introduced the possibility of having computation and other services offered on demand. However, this transformation was not immediately apparent and the scientific community did not immediately recognize its importance, giving scarce support to the Cloud environment with analysis and proposals until recent times (Sriram & Khajeh-Hosseini, 2010). Due to this lack of support, the Cloud made its appearance only recently and was mostly driven by commercial reasons (Mohamed, 2009). The subsequent success of the idea helped create a Cloud environment which grows rapidly in term of services yet shows its limits due to the scalability of legacy infrastructures (Crump, 2010). As a result, the Cloud environment is suffering from scalability and compatibility issues connected to the difficulties of adapting legacy computing and network environments to new requirements and services.

Security in particular has been impacted heavily by the change, and the legacy methods used to ensure authentication, integrity, and privacy are no longer sufficient to cover the new functionalities and the dynamicity of the Cloud (Hu, et al., 2011). In a Cloud environment, where automation plays a primary role, concepts like hardware identity
16 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the product's webpage: www.igi-global.com/chapter/security-cloud-infrastructure/66232?camid=4v1


Recommend this product to your librarian: www.igi-global.com/e-resources/library-recommendation/?id=1

Related Content

**Defining Social Business Process Management: A Delphi Study**
www.igi-global.com/article/defining-social-business-process-management/217440?camid=4v1a

**A Study of the Cascading Effects of Ambulance Diversion among Hospitals**
www.igi-global.com/chapter/study-cascading-effects-ambulance-diversion/72541?camid=4v1a

**Connect Time Limits and Performance Measures in a Dial-Up Modem Pool System**
www.igi-global.com/article/connect-time-limits-performance-measures/39076?camid=4v1a

**A Case Study on Service Oriented Enterprise Interoperability in Automobile Supply Chain**
Yong Zhang, Shijun Liu, Yuchang Jiao and Yuqing Sun (2011). *Service Intelligence and Service Science: Evolutionary Technologies and Challenges* (pp. 201-215).
www.igi-global.com/chapter/case-study-service-oriented-enterprise/47362?camid=4v1a