Chapter 94
Securing Business IT on the Cloud

Bina Ramamurthy
University at Buffalo, USA

ABSTRACT

In this chapter, the author examines the various approaches taken by the popular cloud providers Amazon Web Services (AWS), Google App Engine (GAE), and Windows Azure (Azure) to secure the cloud. AWS offers Infrastructure as a Service model, GAE is representative of the Software as a Service, and Azure represents the Platform as a Service model. Irrespective of the model, a cloud provider offers a variety of services from a simple large-scale storage service to a complete infrastructure for supporting the operations of a modern business. The author discusses some of the security aspects that a cloud customer must be aware of in selecting a cloud service provider for their needs. This discussion includes the major threats posed by multi-tenancy in the cloud. Another important aspect to consider in the security context is machine virtualization. Securing these services involves a whole range of measures from access-point protection at the client end to securing virtual co-tenants on the same physical machine hosted by a cloud. In this chapter, the author highlights the major offerings of the three cloud service providers mentioned above. She discusses the details of some important security challenges and solutions and illustrates them using screen shots of representative security configurations.

1. INTRODUCTION

Security is of utmost concern to the users of cloud computing, understandably so; businesses are typically handing over data, information, computational models, computations, and in many instances the whole IT operation of their organization to a cloud services provider. On the other end, securing the cloud and its resources is all the more critical for the cloud providers, for the survival of their own business. While there are lot of skepticism about the security and trustworthiness of the "cloud" (Chen, 2010), one must understand that the cloud is indeed a composition (combination) of many existing technologies (Reese, 2009). These technologies have successfully used a variety of security measures from basic user authentication to sophisticated PKI based digital certificates (Bishop, 2005). In fact, contrary to common belief, the cloud may offer an effective model for enforcing the security measures uniformly across all applications, data

DOI: 10.4018/978-1-4666-6539-2.ch094

and services hosted by it. It is with this assumption that we approach the discussion in this chapter, where we elaborate on the security challenges and solutions in the existing cloud models. We will examine the approaches to securing the cloud end-to-end, from the perimeter to a processor inner core. Specifically we look at the security models implemented by three of the prominent cloud providers: Amazon Web Services (AWS), Google Cloud Platform (Google) and Windows Azure (Azure). The purpose of the discussion here is to assure the readers that the cloud providers indeed have taken extraordinary measures to secure the cloud and are constantly working on making it even more secure. In this chapter we will focus mainly on AWS security features in detail, along with a few important security features of Google cloud and Windows Azure.

2. BACKGROUND/OVERVIEW

The Internet innovation changed the way computing and information technology being done. When the Internet protocol Version 4 IPV4 was defined by IETF RFC 791 in 1981, nobody anticipated the extent of the growth of the internet (*Limitations, 2013*). It is hard to believe security specifications were not part of this initial RFC. In fact, security was retrofitted by an optional IPSec protocol to secure network communication packets. Security has come a long way since these early days of the Internet. As the major businesses, such as healthcare and education are increasingly getting digital, security plays a critical role in protecting the information privacy and also for assuring the continuity of the businesses. Business consortiums have come up with standards and regulations for security and privacy in their respective domains and cloud providers have been quite eager to comply with these rules and regulations. For instance, all three cloud providers discussed here have been certified by the ISO 27001-standard (*ISO, 2013*) that covers an extensive list of best practices for security management.

3. SECURING THE BUSINESS OPERATIONS ON THE CLOUD

A high level view of the cloud-based system architecture is shown in Figure 1. The client side shown on the left depicts the exponential growth in mobile devices, social networks, and the diversity of application domains. Data generated by these technological advances has been characterized by variety, veracity, high volume and high velocity (the four V's) (Zikopoulis, 2012). Data generated offers a gold mine of intelligence and most businesses desire to take advantage of this. This warrants large and efficient storage and secure access to the data and algorithms. Businesses have been increasingly relying on the cloud to address these newer demands as shown below in Figure 1.

Figure1 shows an organization with the entire IT operations deployed on the cloud; *IT on the cloud* is a popular model among the recent start-ups, with Instagram, Netflix and Pinterest hosting the majority of their operations on the cloud (*Case studies, 2013*). Popular attraction of cloud infrastructure is in the on-demand, quick to install and uninstall, pay-as-you-go provisioning of the common services to support a business. While cloud services may be indispensable for start-ups, it has been an equally popular choice for maintaining legacy services (e.g. 32-bit applications), and for addressing variability in demands at large organizations. Thus the cloud serves a wide range of needs of the modern business organization. A full-fledged commercial cloud provider such as Amazon or Google supports a much richer collection of services than a traditional internal IT department does to the typical average business organization. These extra services demand extra security. Moreover such features as virtualization (Hess, 2010) and co-tenancy of multiple clients on the same network or processors cause an additional level of security issues. We will identify these issues and discuss how these are addressed by the popular cloud providers.