State of Security Readiness

By Ramaswamy Chandramouli and Peter Mell

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. With this pay-as-you-go model of computing, cloud solutions are seen as having the potential to both dramatically reduce costs and increase the rapidity of development of applications.

However, the security readiness of cloud computing is commonly cited among IT executives as the primary barrier preventing organizations from immediately leveraging this new technology. These problems are real and arise from the nature of cloud computing: broad network access, resource pooling, and on-demand service.

In this article, we survey some of these challenges and the set of security requirements that may be demanded in the context of various cloud service offerings (noted in the article as No. 1, No. 2, and so on). The security challenges and requirements we survey not only involve core security operations, such as encryption of data at rest and in transit, but also contingency-related operations, such as failover measures.

The survey touches upon the various artifacts or entities involved in IT services, such as the users, data, applications, computing platforms and hardware. We call the enterprise or government agency subscribing to the cloud services as the "cloud user" and the entity hosting the cloud services as the "cloud provider."

To further refine the definition of cloud computing presented above, we classify cloud computing service offerings into three service models.

Service Models

Software as a service (*SaaS*). The capability provided to the consumer is the use of a provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. Examples of this include the case of a cloud provider offering a software application used for a specific business function, such as customer relationship management or human resources management, on a subscription or usage basis rather than the familiar purchase or licensing basis.

Platform as a service (*PaaS*). The capability provided to the consumer is the deployment of consumer-created or acquired applications onto the cloud infrastructure. These applications are created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations. Examples of this include the case of a cloud provider providing a set of tools for developing and deploying applications using various languages (for example, C, C++, Java) under a whole application framework (JEE, .NET, and so forth).

Infrastructure as a service (*IaaS*). The capability provided to the consumer is provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (for example, host firewalls). Examples of this include the case of a cloud provider providing physical and virtual hardware (servers, storage volumes) for hosting and linking all enterprise applications and storing all enterprise data—in other words, the infrastructure backbone for an enterprise's data center.

Survey of Security Challenges

In reviewing the security challenges and requirements of cloud computing, we will look first at the necessary interactions between the cloud users, the users' software clients, and the cloud infrastructure or services.

The Users

When an enterprise subscribes to a cloud service, it may have a diverse user base consisting of not only its own employees but also its partners, suppliers, and contractors. In this scenario, the enterprise may need an effective identity and access management function and therefore require the following security requirements:

- support for a federation protocol for authentication of users (No. 1) and
- support for a standardized interface to enable the cloud user (or the cloud user's system administrator) to provision and de-provision members of their user base (No. 2).

Many commercial cloud services are now beginning to provide support for the security assertion markup language (SAML) federation protocol (which contains authentication credentials in the form of SAML assertions) in addition to their own proprietary authentication protocol, and hence we do not see a big obstacle in meeting the first of the above requirements.

As far as the user provisioning and de-provisioning requirement is concerned, many of the cloud providers still use their own proprietary interfaces for user management. There exist common, machine-neutral formats or XML vocabularies for expressing user entitlements or access policies, such as the extensible access control markup language (XACML), and for user provisioning and de-provisioning with capabilities such as the service provision markup language (SPML). Until the user management interface of the cloud provider provides supports for these kinds of protocols, the cloud user's control of this important security function cannot be realized.

Access to Data

Data is an enterprise's core asset. What are the security challenges and requirements surrounding access to data stored in the cloud infrastructure?

Driven by citizen safety and privacy measures, government agencies and enterprises (for example, healthcare organizations) may demand of a SaaS, PaaS, or IaaS cloud provider that the data pertaining to their applications be:

- hosted in hardware located within the nation's territory or a specific region, for example, for disaster recovery concerns (No. 3), and
- protected against malicious or misused processes running in the cloud (No. 4).

For many cloud providers, hosting hardware within a specific region can be done easily. However, protecting the data itself from malicious processes in the cloud is often more difficult. For many cloud providers, the competitiveness of the service offering may depend upon the degree of multi-tenancy. This represents a threat exposure as the many customers of a cloud could potentially gain control of processes that have access to other customers' data.

> “Security readiness is commonly cited among IT executives as the primary barrier preventing organizations from immediately leveraging cloud computing.”

Given the challenges in protecting access to cloud data, encryption may provide additional levels of security. Some enterprises, due to sensitive or proprietary nature of data and due to other protection requirements such as intellectual property rights, may need to protect the confidentiality of data and hence may require that both data in transport and data at rest (during storage) be encrypted (Nos. 5 and 6).

While encryption of data in transit can be provided through various security protocols such as transport layer security and web services-security based on robust cryptographic algorithms, encryption of data at rest requires the additional tasks of key management (for example, key ownership, key rollovers, and key escrow). The cloud environment has a unique ownership structure in the sense that the owner of the data is the cloud user while physical resources hosting the data are owned by the cloud provider. In this environment, best practices for key management have yet to evolve, and this is one of the areas the standard bodies or industry consortiums have to address in order to meet the encryption requirements of data at rest.

Data protection, depending upon the criticality of data, may call for either periodical backups or real time duplication or replication. This is true in any enterprise IT environment. Hence the cloud user has to look for these capabilities in an IaaS provider offering storage service. We will call this subclass of IaaS cloud provider a cloud storage provider.

Further, if the cloud storage provider has experienced a data breach or if the cloud user is not satisfied with the data recovery features or data availability (which is also a security parameter) provided by that organization, the latter should have the means to rapidly migrate the data from one cloud storage provider to another.

In some cases, the data protection may also call for capabilities for segmenting data among various cloud storage providers. As a result, secure and rapid data backup and recovery capabilities should be provided for all mission-critical data (No. 7), and common APIs should be required to migrate data from one cloud storage provider to another (No. 8).

Vulnerabilities for PaaS

When developing applications in a PaaS cloud environment, especially for PaaS solutions, what might leave the application security vulnerable? Vulnerabilities represent a major security concern whether applications are hosted internally at an enterprise or offered as a service in the cloud.

In the cloud environment, the custom applications developed by the cloud user are hosted using the deployment tools and run time libraries or executables provided by the PaaS cloud provider. While it is the responsibility of cloud users to ensure that vulnerabilities such as buffer overflows and lack of input validation are not present in their custom applications, they might expect similar and additional properties, such as lack of parsing errors and immunity to SQL injection attacks, to be present in the application framework services provided by a PaaS cloud provider.

Additionally, they have the right to expect that persistent programs such as web servers will be configured to run not as a privileged user (such as root). Further, the modern application frameworks based on service oriented architectures provide facilities for dynamically linking applications based on the dynamic discovery capabilities provided by a persistent program called the Directory Server. Hence this directory server program also needs to be securely configured.

Based on the above discussion, two security requirements may arise from cloud users. First, the modules in the application framework provided are free of vulnerabilities (No. 9). Second, persistent programs such as web servers and directory servers are configured properly (No. 10).

The biggest business factors driving the use of IaaS cloud providers is the high capital costs involved in purchase and operation of high performance servers and the network gears involved in linking up the servers to form a cluster to support compute-intensive applications. The economy of service offered by an IaaS cloud provider comes from the maximum utilization of physical servers and hence it is difficult to think of an IaaS cloud offering without a virtual machine.

While it's critical in PaaS to offer services to ensure the security of developed applications, in IaaS it's critical for the cloud provider to rent to the users secure operating systems. IaaS cloud providers usually offer a platform for subscribers (cloud users) to define their own virtual machines to host their various applications and associated data by running a user-controlled operating system within a virtual machine monitor or hypervisor on the cloud provider's physical servers. In this context, a primary concern of a subscriber to an IaaS cloud service is that their virtual machines are able to run safely without becoming targets of an attack, such as a side channel attack, from rogue virtual machines collocated on the same physical server.

If cloud users are not satisfied with the services provided by the current cloud provider due to security or performance reasons, they should have the capability to de-provision the virtual machines from the unsatisfactory cloud provider and provision them on a new cloud provider of their choice. Users may need to migrate from one virtual machine to another in real time, so as to provide a seamless computing experience for the end users.

These needs translate to the following security requirements:

- the capability to monitor the status of virtual machines and generate instant alerts (No. 11),
- the capability for the user to migrate virtual machines (in non-real time) from one cloud provider to another (No. 12), and
- the capability to perform live migration of VMs from one cloud provider to another or from one cloud region to another (No. 13).

Tools to continuously monitor the vulnerabilities or attack on virtual machines running on a server have already been developed or are under development by many vendors, and hence the first of the above requirements can be easily met. Large scale adoption of virtual machine import format standards such as open virtualization format will enable the user to rapidly provision virtual machines into one cloud provider environment and de-provision at another cloud provider environment which is no longer needed by the cloud user and thus meet the second requirement above.

Further, a virtual machine migrated using a common import format should not require extensive time to reconfigure under the new environment. Hence common run time formats are also required to enable the newly migrated virtual machine to start execution in the new environment. Live migration of virtual machines (in situations of peak loads) is now possible only if the source and target virtual machines run on physical servers with the same instruction set architecture. The industry is already taking steps to address this limitation. However, since the majority of virtualized environments run the x86 ISA, this is not a major limitation.

Standards

With respect to standards and cloud security readiness, we have made four major observations.

First, some requirements are already met today using existing standards (such as Federation protocols for authentication) and technologies (automatic real-time duplication of data for disaster recovery). Second, some requirements can be met if there is more market support for existing standards (XACML and SPML for user provisioning, open virtualization format for virtual machines migration). Third, some requirements such as data location and non multi-tenancy can be met by restructuring cost models for associated cloud service offerings. And fourth, some requirements can only be met by developing new standards (common run time formats for virtual machines, common APIs for migration of data from one cloud storage provider to another).

While cloud computing presents these challenges, it has the potential to revolutionize how we use information technology and how we manage datacenters. The impact may be enormous with respect to IT cost reduction and increased rapidity and agility of application deployment. Thus, it is critical that we investigate and address these security issues. While some issues may have ready answers (such as existing security standards), others may be more problematic (such as threat exposure due to multi-tenancy).

The ultimate answer is almost certainly multifaceted. Technical solutions will be discovered and implemented. Security standards will enable new capabilities. Finally, differing models and types of clouds will be used for data of varying sensitivity levels to take into account the residual risk.

Biographies

Dr. Ramaswamy Chandramouli is a supervisory computer scientist in the Computer Security Division, Information Technology Laboratory at NIST. He is the author of two text books and more than 30 peer-reviewed publications in the areas of role-based access control models, model-based test development, security policy specification and validation, conformance testing of smart card interfaces and identity management. He holds a PhD in information technology security from George Mason University.

Peter Mell is a senior computer scientist in the Computer Security Division at the NIST, where he is the cloud computing and security project lead, as well as vice chair of the interagency Cloud Computing Advisory Council. He is also the creator of the United States National Vulnerability Database and lead author of the Common Vulnerability Scoring System (CVSS) version 2 vulnerability metric used to secure credit card systems worldwide.