Auditing for Standards Compliance in the Cloud: Challenges and Directions

Hassan Rasheed
AUDITING FOR STANDARDS COMPLIANCE IN THE CLOUD: CHALLENGES AND DIRECTIONS

HASSAN RASHEED
DEAN, INFORMATION TECHNOLOGY, TAIF UNIVERSITY, SAUDI ARABIA

Abstract:
Cloud computing has recently grown into prominence as one of the most attractive computing paradigms used for businesses to cut costs, while simultaneously gaining the ability to dynamically allocate the technology resources that meet their needs. Despite its attractiveness, however, many organizations remain reserved due to concerns about the security and auditability of cloud environments. In this paper, we evaluate some of the unique security challenges created by cloud computing and how these challenges impact auditing towards standards compliance. We examine the notion of audit as it is currently being used by surveying available provider APIs and new standards for publishing audit data. Our research has concluded that, while there are some promising efforts underway, current efforts by cloud providers being termed as audit, still fall short of addressing some of the most pressing concerns of their customers related to multiple issues.

Keywords: Cloud Computing, Audit, IT Standards Compliance.

1. INTRODUCTION

The solidification of cloud computing as one of the most popular computing paradigms today, has not removed the concerns that many hold related to the level of security provided to customers. The capability to audit systems deployed on cloud architectures is simultaneously one of the most pressing security concerns and one of the most difficult to resolve, due to the manner in which most cloud systems are architected. A recent report by the European Network and Information Security Agency [17] listed concerns regarding cloud computing security. Among the top ten risks, two of them - loss of governance and compliance risks - were traced to the same vulnerability: namely, that audit is not available to customers.

Achieving compliance with an IT security standard and successfully undergoing the auditing procedure for such a standard while utilizing public cloud computing architectures is a daunting proposition causing many organizations to hold back from adopting cloud services. Organizations must confront standards whose language often does not encompass the technologies underpinning cloud computing as well cloud providers who have not standardized the necessary security measures in their cloud offering and do not make the necessary type of audit information available to customers.

2. INTRODUCTION TO CLOUD COMPUTING

Cloud computing has become a compelling business model for companies owning large data centers to essentially rent out different portions of their computing resources. This has emerged in large part because many companies now rely internally on technologies that must be able to scale dynamically and they rely on large sets of homogeneous hardware for their processing. These organizations have developed a high level of proficiency deploying scalable applications over virtualized architectures with commodity hardware to the extent that they can easily provide these resources as a service to others. This is often known is the field of economics as economies of scale.
When economies of scale are achieved, companies achieve the ability to provide a service to consumers cheaper than it would be for the consumer to make that same resource internally within their own organization. And thus, organizations have found they can reduce IT costs by merely outsourcing one or more types of their internal IT infrastructure to a cloud service provider.

The National Institutes of Standards and Technology (NIST) have formalized these services being offered to consumers into three different types: Platform as a Service, Infrastructure as a Service, and Software as a Service [13].

At the most basic hardware level, Infrastructure as a Service (IaaS) is the model where a service provider makes a set of virtualized hardware components (such as virtual machines or networked storage) available to consumers, which can be used to build and run applications. Each of these hardware components is visible to the consumer. An example of an Infrastructure as a Service (IaaS) offering is Amazon EC2 [2] which allows customers to dynamically provision new virtual machines on the Amazon cloud either from templates or with their own custom settings.

At the next highest level, Platform as a Service (PaaS) occurs when a service provider or vendor offers an entire runtime environment for an application to a client. This would include the basic hardware in addition to critical libraries that the customer’s application will rely on. The underlying hardware, however, is not visible to the user and they do not have the same level of control over those resources as IaaS customers do. An example of PaaS is Google AppEngine [7] which allows developers to make use of some of the same tools and libraries used in Google web application, to build their own custom applications by building on a common application platform.

At the highest level is Software as a Service (SaaS), which occurs when a cloud provider provides consumers with the use of an application running on its servers. The consumer only views the specific application features that the service provider surfaces for them. An example of Software as a Service is the Salesforce.com application [16] which provides consumers with customer relationship management software.

3. AUDIT FOR COMPLIANCE TO INDUSTRY STANDARD

Many of the most stringent audit requirements of concern, within the realm of cloud computing, are due to the need for organizations to provide evidence for compliance with security standards such as Payment Card Industry Data Security Standard (PCI DSS) [14] and International Standards Organization Data Security Standard ISO 27002/17799 [10]. Although a detailed analysis of either of these standards is beyond the scope of this work, a few of the common requirements that are difficult within a cloud environment will be highlighted here.

The relationship between the cloud service provider and their clients has raised the question of which of the two is responsible for achieving compliance. In some cases, organizations have turned to solutions centered on outsourcing credit card processing to third parties, in an effort to simultaneously meet PCI guidelines and continue hosting their applications with public cloud providers [3]. We will examine the PCI DSS, as an example of the challenges faced when trying to achieve standards compliance while using public cloud services.

3.1 OVERVIEW OF PCI DSS

PCI DSS [14] is one of most frequently referred to standards in IT, because certification of adherence to its tenants is necessary for an organization to be certified to store and process customer credit card information. The standard contains 11 core requirements in six main areas: building and maintaining a secure network, protecting cardholder data, maintaining a vulnerability management program, implementing strong access control measures, regularly monitoring and testing networks and maintaining an information security policy.
Organizations wishing to gain certification against the requirements of this standard must get an assessment from a security specialist approved by PCI DSS.

Recent reports [8] indicate varying answers from security specialists regarding the question of whether or not it is possible to achieve PCI compliance when using public cloud services. The answers seem to vary in part because adherence to the PCI standard is based on the subjective judgment of a certified security specialist and the standard itself was not written with cloud-like virtualized architectures in mind. This would seem to indicate there is no consensus among the security community regarding how to map older security techniques such as network separation and perimeter security into the emerging application architectures seen frequently with cloud service providers [15].

This most recent version of the PCI DSS (v2.0) added language explicitly clarifying that virtual components are also included under the heading of system components to which the standard applies. It also makes allowances for multi-tenant virtual architectures in that the previous requirement for each server to implement only one primary function has been adapted to allow for a single hardware server to effectively host multiple virtual machines with different functions as long as each of the virtual machines has only one primary function.

3.2 PCI REQUIREMENTS PROBLEMATIC IN CLOUD ENVIRONMENTS

A recent white paper by a group of industry organizations including HyTrust, Cisco, Coalfire, Savvis and VMware [15] recommended an architecture that would theoretically allow organizations using private cloud architectures to achieve PCI compliance. The reference architecture is essentially pieced together from the various technology solutions offered by the document authors. The paper is organized as an analysis of the PCI standard from the perspective of noting which requirements would be difficult to satisfy in a cloud computing environment. After discussing each risk, various technologies offered by the document authors are discussed as potentially solutions which mitigate the risks which were raised. Although many of the risks cited are somewhat ambiguous and there are a few that provide insight into the unique security requirements of virtualized deployments, the risks raised in the paper can be divided into the following categories:

- Virtualized Network Devices
- Automatic Provisioning of New Systems
- Storage of Volatile Memory on Disk
- Data Disclosure of Private Data on Public Networks
- System Vulnerability Management
- Access Control
- Tracing and Logging of System Activity

The first challenge is in fulfilling the requirement to install and maintain a firewall configuration to protect cardholder data. The difference between traditional network deployments and cloud deployments is that virtual and cloud environments rely on virtualized network devices (network interfaces, switches and firewalls) to provide segmentation. This places a greater burden for documentation on the organization undergoing the PCI audit to demonstrate how the parts of their infrastructure help them to achieve compliance. In some cases it can be more complex to perform a thorough inspection of a virtual architecture than a physical one where network separation can be demonstrated very easily. In the case of this requirement, that would mean documenting how the virtual firewall is installed and maintained and how the virtual network space is partitioned.

Automatic provisioning of new systems presents two challenges with regards to the PCI requirements. The first is that frequently automatically provisioned systems are created with default settings (this is the second risk mentioned in the white-paper) whereas the PCI standard requires that organizations not use vendor supplied defaults for system passwords and other security parameters. The second security risk arising from automatic provisioning, which is essentially lack of anti-virus protection, is easier to resolve and only arises if the solution being used for automatic provisioning does not support the installation, update and monitoring of
anti-virus on all deployed systems, as required in the PCI standard. There are currently many systems on the market that provide a company with the ability to monitor and automatically their anti-virus installations across an enterprise, but few of those products may be well integrated with the system responsible for provisioning new virtual images.

The third risk mentioned arises from the new capability to write previously volatile memory to disk by taking snapshots of systems. This risk relates to the requirement to protect stored cardholder data. Previously in-memory data now being written to disk could be at a greater risk for disclosure to unauthorized parties without proper access controls. The solutions proposed in the HyTrust reference architecture, therefore, revolve around maintaining strict access control for stored images and encrypting their backups.

The PCI specification also requires that any cardholder data transmitted across public networks is encrypted. There is a potential risk to this requirement in cloud systems, depending on whether or not any part of the cloud network being utilized is considered a public network. In private cloud systems, this requirement is more easily satisfied as encryption would only need to occur when transmitting cardholder data to third parties. Based on the recent recognition of virtualized components by the PCI standard, virtual devices could potentially be used to even privatize a network hosted on an otherwise public cloud provider.

Requirement six which broadly requires the development and maintenance of secure systems has more detailed provisions concerning ensuring that the latest security patches are applied and that the organization has a process in place to identify and assign risk to newly discovered security vulnerabilities. The reference architecture addresses part of this requirement by mentioning the capability of VMware Update Manager to deploy patches, although this is likely limited to operating system software that is deployed and configured by the VMware management infrastructure from the beginning. Other application patching and updating will likely follow a work-flow unchanged from the one the organization would use with non-virtualized deployments.

Requirements seven through nine all center around the notion of access control. Restriction of access to cardholder data on a need-to-know basis is the subject of requirement seven. The two main sub-requirements, therefore, concern access limitation based on job function and establishment of a access control system that defaults to deny-all and restricts permissions based on the user’s need to know. The additional difficulty being introduced here is that in a heavily virtualized architecture, the dependency on the virtual hypervisor for provisioning systems, application and even virtual networked components makes it difficult to use traditional access control mechanisms that might work only at the application level or only at the network level. It is essential, therefore, that highly virtualized environments in need of strong access control solutions find one that integrates well with the chief virtualization component being used. In requirement eight it is specified that users accessing machines must use a unique identifier - this essentially necessitates an authentication process where each user is assigned a distinct account. Requirement nine pertains to physical access controls and thus is out of scope of a software solution.

Requirement ten stipulates that entities processing cardholder data must maintain audit traces for all machine activity. This functionality is normal at the operating system and application levels, but must also be built into the system that manages virtual systems and components. There is also the additional issue of activity logs being preserved and available for audit when machines are deactivated either permanently or temporarily. The solutions proposed in the HyTrust framework essentially address maintaining logs of administrative activity at the system and network levels. The final requirement that places unique constraints on virtualized systems is requirement number 11 which mandates regular tests for security systems and processes. Although there are many vulnerability scanning products on the market which would even be sufficient for virtual systems, it would be important for such systems
to ensure that virtual systems being dynamically provisioned are also monitored and tested.

While this reference architecture may resolve some of the problems with securing the cloud, it only does so in a private cloud architecture where the organization is willing to deploy these necessary technologies to meet the requirements. Organizations utilizing public cloud offerings where they have no control over the infrastructure and deployment of security controls will still have to find other solutions if they are seeking PCI compliance.

4. AUDIT FACILITIES OFFERED BY CLOUD PROVIDERS

In the previous section, we reviewed some of the challenges related to achieving standards compliance while using cloud computing services. The focus was on the inherent difficulties presented by the standards themselves.

In this section, we look at some additional challenges introduced by the lack of audit data made available by the cloud service provider. We examine a current, industry-leading audit API in the Amazon CloudWatch API [1] as an example of the highest level of audit data that customers can currently expect from a cloud provider. We also examine CloudAudit, a relatively new standard under development which would provide a common interface allowing interested cloud providers to give their customers more detailed audit information.

4.1 A CASE STUDY ON THE AMAZON CLOUDWATCH API

One of the more developed frameworks for analysis and audit of purchased cloud resources is the Amazon CloudWatch API [1]. The CloudWatch API operates multiple varied services that fall under the heading of Amazon Web Services. This API provides consumers with statistical data on the performance of the server instances they are currently running with Amazon Web Services (AWS). We will outline the auditing capability available for Amazon Elastic Compute Cloud (EC2) and Elastic Load Balancing (ELB). The Amazon Relational Database Service (ARDS) also offers similar capabilities, but they will not be discussed here.

Some AWS services send updated information to CloudWatch every five minutes and others send that information every minute. The CloudWatch API divides statistical information into metrics, which are specific measurable system properties. Different services provide different metrics based on the nature of the service. There are also four aggregate operations which can be used to tailor calculation of the metrics: minimum, maximum, sum and average, although not all operations are available with each metric. One limitation of the CloudWatch API is that the information it provides is region-specific and customers must perform additional processing if they want to aggregate data across deployments in multiple regions.

EC2 is a web service that allows customers to dynamically provision virtual machines with varying configurations on the Amazon cloud infrastructure. New instances can be created using templates or by creating a machine image and specifying its application, libraries and settings. There are seven metrics that are available from EC2, divided into the following categories:

- CPU Usage - measures the percentage of allocated compute units that are currently in use on the instance.
- Network I/O Statistics - two measures summarizing the total number of bytes sent and received on all network interfaces associated with the instance
- Disk I/O Statistics - four measures which summarize completed read and write operations and total bytes written to and read from disk

Amazon Elastic Load Balancing is an additional service that runs on top of EC2 and allows the customer to dynamically route traffic to various compatible EC2 instances to distribute the traffic and processing load. Four Metrics are available from Elastic Load Balancing:
Latency: Time taken between a request and the corresponding response as seen by the load balancer

Request Count: The number of requests processed by the LoadBalancer

Host Health - two different measures that provide counts of the number of healthy and unhealthy hosts respectively

Amazon’s CloudWatch API provides a significant set of data on resource usage and server performance for consumption by the cloud service consumer. Many of these metrics would likely be collected by Amazon anyway for billing purposes - the API just provides another service to customers and another opportunity for Amazon to monetize their existing monitoring infrastructure by having clients pay for accessing certain types of data. In addition, to some degree it mitigates the lack of direct monitoring control over systems in the cloud by giving customers some low-level information which would be essential for monitoring and adjusting deployments.

The provided metrics, however, do not ameliorate concerns regarding the level of audit that the cloud service provider makes available to consumers. Few, if any, of the questions raised during a PCI audit, for example, could be answered by the data provided in the CloudWatch API. The primary use of this type of data is for customers to evaluate the performance of their applications and systems and possibly troubleshoot performance issues that are showing up on the systems front end. An example of such a use case would be an organization with an application running on several systems hosted the Amazon EC2 service. If they begin to get reports of slow application response time during a specific period, they could compare the metrics gathered through the CloudWatch API during that period with some previous baseline data as a starting point in looking for performance anomalies.

4.2. CLOUD AUDIT API

The Cloud Audit Working Group [6] is a relatively recent effort, which began in January 2010 and submitted an Internet Engineering Task Force (IETF) standard draft for an API in July 2010 [9]. The working group responsible for the standard consists of members from over 250 companies and organizations. The core members, and those responsible for the internet draft, are members of Cisco Systems, Google, enStratus and TELUS. The draft proposes a standard API for cloud providers to use in making “Audit, Assertion, Assessment, and Assurance” information available to third parties including customers and auditors. The standard essentially covers conventions for cloud computing providers to create groups of various documents that are accessible via HTTP at standardized URLs. The basic standard covers how data is stored and retrieved and how errors are handled and is extendable to cover specific audit standards.

<table>
<thead>
<tr>
<th>Specifications</th>
<th>Namespace URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCI DSS v1.2.1 2.4</td>
<td>./well-known/cloudaudit/org/pcisecuritystandards/DSS/1-2-1/2-4/</td>
</tr>
<tr>
<td>PCI DSS v1.2.1 12.8</td>
<td>./well-known/cloudaudit/org/pcisecuritystandards/DSS/1-2-1/12-8/</td>
</tr>
<tr>
<td>PCI DSS v1.2.1 12.8.1</td>
<td>./well-known/cloudaudit/org/pcisecuritystandards/DSS/1-2-1/12-8-1/</td>
</tr>
<tr>
<td>PCI DSS v1.2.1 12.8.2</td>
<td>./well-known/cloudaudit/org/pcisecuritystandards/DSS/1-2-1/12-8-2/</td>
</tr>
<tr>
<td>PCI DSS v1.2.1 12.8.4</td>
<td>./well-known/cloudaudit/org/pcisecuritystandards/DSS/1-2-1/12-8-4/</td>
</tr>
</tbody>
</table>

Figure 1. A Sample of Specifications Within the PCI DSS Standard and the URL Namespaces that they are mapped to by the CloudAudit PCI Compliance Pack.
Each standards compliance framework is mapped to a set of namespaces. The namespaces for a specific standard are intended to organize documents that give detailed information on the way in which the cloud provider addresses the requirements of that particular standard or auditing framework. The namespace is specified by a standardized URL which contains the domain of the organization providing the information, the name of the standard and its version. Each sub-requirement in a compliance or audit standard is represented with an extension of the base namespace URL such that the various documents applying to a single standard can be accessed and updated in an automated way if desired.

The draft discusses the notion of “compliance packs” which will be used to describe the data and metadata useful within specific audit and compliance frameworks. As of the time of this writing, compliance packs had been made available for the following frameworks: COBIT, HIPAA, ISO 27002, PCI and NIST 800-53. In the current version, the compliance packs are spreadsheets which map requirements within the standard to a namespace or URL at which the cloud provider supporting the standard should provide documentation on their compliance with its requirements. An excerpt of the compliance pack for PCI DSS is shown in Figure 1.

The presence of a standard way for service providers to present information on standards compliance is not, on its own, an assurance as to if and when such information will actually start being made available. As we have highlighted by looking at what could arguably be called the current industry leading API for audit information (Amazon’s Cloud Watch API), the type of information which would be presented under the CloudAudit API is not currently being made available by providers at all, let alone in a standardized manner. In addition, while the Cloud Audit API might standardize methods for accessing standards-compliance documentation, the content of that documentation is outside the scope of the work. As a result, even in the event that cloud providers begin implementing the CloudAudit API there is still some question as to whether or not they will be willing to provide the kind of detail on their infrastructure sought by auditors.

Adoption of the standard for data presentation by the cloud service providers would not necessarily alleviate all of the audit concerns. It would, however, at least begin to provide customers with access to the data. It would also provide customers with criteria to differentiate cloud providers based on the amount and detail of the information which they provide. This will enable customers to make an informed decision when selecting a cloud provider, so that they can partner with companies which will make it easier for them to achieve standards compliance. It is also likely that when audit information provided to customers begins to be a differentiating factor, market forces will subsequently drive companies to continue to improve in this area.

5. RELATED WORK

There are two areas related to the issue of auditing clouds for standards compliance. Those areas are general cloud security and theoretical approaches for examining and auditing data stored remotely. In [5] the authors provide an overview of the security issues in the area of cloud computing, proposing taxonomy of traditional security issues that are also problematic in cloud computing, but also detailing a few new security problems introduced by the nature of the cloud computing paradigm and its related technologies. The authors in [4] perform a similar analysis, arguing that most of the security issues related to cloud computing were first confronted in the main-frame time-sharing computing era but that multi-party trust and the need for mutual auditability are security issues unique to the current formulation of cloud computing. The research presented in [12] examines some of the legal and regulatory issues over whether the customer or the cloud service provider is responsible for maintaining data security for information stored in the cloud. In [11] the author surveys the security and privacy issues related to cloud computing and provides some guidelines for organizations considering utilizing cloud service offerings. Wang et al. [18] propose a technique to allow third parties to
verify the integrity of data stored in the cloud, focusing on doing so while preserving the privacy of the data and simultaneously allowing dynamic data updates.

6. CONCLUSION

The lack of service-provider supported interfaces for customers to audit the security of their provisioned systems remains a significant shortcoming blocking adoption of public cloud offerings for many organizations. Although the standards themselves have begun to adapt, there are also many provisions of the standards that are incompatible with the newly emerging paradigm of cloud computing. In examining the PCI DSS standard, some of the unique challenges to achieving compliance while relying on public cloud offerings were shown. Two industry efforts - the Cloud Watch API and the CloudAudit API - were profiled in order to establish the current state of cloud-provider supported audit and the new directions being pursued to expand the scope of available audit data in the near future. Progress in this area will ultimately be the result of all of the stakeholders making adjustments in their respective areas: standards organizations must update their requirements to allow for things like virtualized networking components while reformulating the notion of data security to accommodate emerging computing paradigms. Cloud providers must begin to make more audit data available to customers and possibly even provide hosting solutions specifically geared towards meeting the needs of customers seeking standards compliance.

REFERENCES:


Institutes of Standards and Technology (NIST), Gaithersburg, MD, January 2011.


