A Survey of Cloud Security Issues and Offerings

Michael J. Schultz, mjschultz@gmail.com (A project report written under the guidance of Prof. Raj Jain)

(A project report written under the guidance of Prof. Raj Jain) Download

Abstract

Cloud computing is a recent trend in computing because it offers dynamic, low-cost computing solutions. However, it also introduces new problems with data security, privacy, authorization, and availability that were not as apparent as before.

This paper does not aim to provide a comprehensive solution to those problems but rather enlighten the reader as to what problems do or can exist when using cloud computing. From this knowledge, the reader should be able to make informed decisions and be aware of what obligations the cloud customer takes and what security measures the cloud provider must use to ensure secure computing on their service.

Keywords

Cloud computing, cloud security, Amazon Web Services, Google Apps, Windows Azure Platform, cloud providers, cloud standards, cloud attacks, software as a service, SaaS, platform as a service, PaaS, infrastructure as a service, IaaS

Table of Contents

1 Introduction

The concept of cloud computing has taken off recently as the next big thing in computing. Because the "cloud" is new, the terminology is largely ill-defined and it can be difficult to determine what the cloud does and does not include. This paper defines the three commonly accepted cloud services: software as a service, platform as a service, and infrastructure as a service. Using these definitions a clear separation of security concerns between a cloud customer and a cloud provider can be built.

Section 2 presents security issues that have already manifested in cloud computing. These problems serve as concrete motivation for concern and to demonstrate that there is need for both customers and providers to take security seriously. Security is a complex issue and it is not the sole responsibility of the provider nor is it the sole responsibility of the customer.

To make the provider and customer responsibilities explicit, Section 3 looks at who is in control of what at different layers of the cloud ecosystem. It is also important to discuss data ownership issues and potential attack possibilities that come up when working in a cloud environment. Section 4 extends this discussion by looking at actual cloud providers and the steps they have taken to protect the cloud platforms that are in use.

1.1 Definitions

Before delving too deeply into what cloud security means, the term "cloud" must be carefully defined to avoid any ambiguity in what it means. There are many providers of cloud services, each seeming to offer different services to the customer and in some cases the services seem to be completely opposite of each other. In the following sections, the types of cloud services (software, platform, and infrastructure) are defined and then the types of clouds (private, community, public, and hybrid) are discussed.

1.1.1 Cloud Services

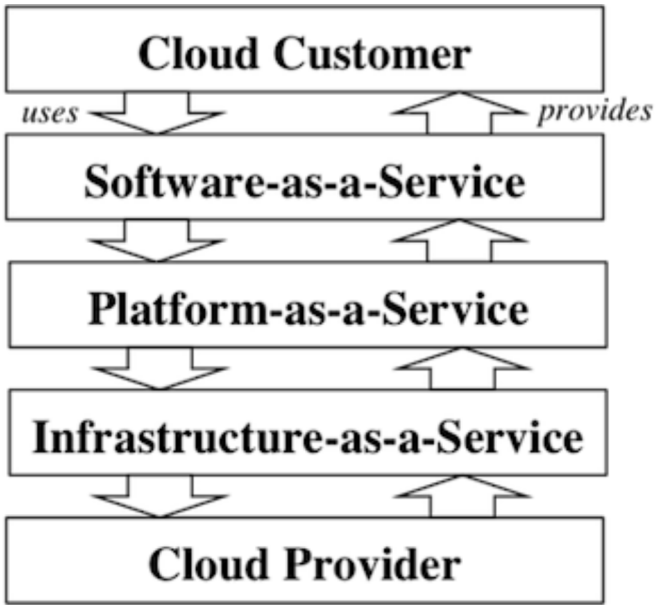

Figure 1: The relationship between a cloud customer and a cloud provider can go through several layers.

As shown in Figure 1, a cloud customer and cloud provider can meet at any cloud service layer. Each layer defines an entity that performs some function that can use the layer below it and can provide a service to the

layer above. These layers correspond to a logical separation between what a customer wants to be concerned with and what should "just work."

Software as a Service (SaaS) places the separation very high in the stack where the customer is simply an end-user and requires only a web browser [NIST800-145]. For example, a web-based email client is a SaaS where the customer does not need to install or configure their email client. All the details about mail transfer, delivery, storage, and spam filtering are provided to the customer as a service with some relationship agreement in place.

Platform as a Service (PaaS) moves the separation lower in the stack where the customer is a software developer. As with SaaS, the PaaS customer does not want to pay attention to the underlying details of purchasing a computer, installing the operating system, selecting a web server, and gathering all the dependencies for running the software [NIST800-145]. Rather, the software developer wants the entire platform provided as a service to use, allowing the focus to be solely on the software being developed.

Infrastructure as a Service (IaaS) takes the separation even lower and provides the developer with the physical infrastructure needed to provide a service. Thus, the service provider controls the physical resources (networking equipment, connectivity, and physical hardware), while the developer would have control of anything above those resources [NIST800-145]. The provider typically allows the developer to create virtual machines on the physical resources, giving the developer complete control of the system from the choice of operating system to the choice of web environment.

1.1.2 Cloud Types

Separate from the various services cloud computing provides are four different types of clouds: private, community, public, and hybrid [NIST800-145]. A **private** cloud is one dedicated to the customer. These clouds are internal to an organization and cannot be directly accessed from the outside. For example, many universities have their own compute clouds for running scientific routines to keep potentially sensitive data within the university. **Community** clouds are similar to private clouds. Instead of a single organization using the cloud, several organizations pool their resources together and operate the cloud jointly. An example of a community cloud is the Southeast Wisconsin High Performance cyberinfrastructure, which mandates that member institutions provide compute resources in exchange for access to more compute power [SeWHiP11]. **Public** clouds are those that anyone in the public has access to by purchasing computation units from a cloud provider like Amazon Web Services or Google App Engine. Finally, **hybrid** clouds are clouds that make use of a combination of the previous three cloud types. Hybrid clouds can be useful if a company wants to outsource certain aspects of their workloads to a public provider while still keeping other parts wholly internal.

From a security perspective all these cloud types should be treated in the same manner. [Golden11] Though it may be widely believed that a private cloud is more secure than a public cloud, this cannot be guaranteed. An organization that has both the resources and need to build a private cloud likely has multiple applications that need to share the services provided by the cloud. The data may stay within the organization, but if strict security measures are not in place or not enforced that data may fall into the hands of unauthorized users. The safest way to ensure this does not happen is to treat the cloud as if it were a public resource and to not assume there is "built-in" security.

1.2 Organizations

Now knowing the definitions for cloud computing services (SaaS, PaaS, and IaaS), it is useful to have concrete examples of cloud providers and the type of services they offer. This is not a comprehensive list of cloud providers, but rather a list of common providers that a reader may recognize or use. Similarly, there are

organizations that strive to provide standards to which cloud providers should conform. These organizations are not necessarily unique to cloud computing but do provide audits or assurances to customers that the cloud provider follows certain regulations.

1.2.1 Cloud Service Providers

Since there are a multitude of cloud service providers, this section focuses on a few providers in each of the infrastructure-, platform-, and software as a service layers.

Starting at the lowest layer, infrastructure as a service, providers include: Amazon Elastic Compute Cloud (Amazon EC2) [Amazon11a], Rackspace Cloud (formerly Slicehost) [Rackspace11], and IBM SmartCloud [IBM11]. Each of these IaaS providers allow the customer to run their own operating system to configure as needed. They also provide various other related services such a storage, database, and messaging.

At the middle layer, platform as a service, providers include: Google App Engine (GAE) [Google11a], Heroku [Heroku11], and Windows Azure Platfrom [Azure11]. The distinction between IaaS and PaaS providers can be difficult to see clearly because most IaaS providers also have PaaS solutions. However, the common ground among PaaS providers is that they provide a programming platform instead of bringing your own. This frees the customer from securing their own operating system instances and allows them to focus on the application details. These companies all provide some programming and run-time environment (i.e. Ruby, Python, .NET Framework, etc.) and also provide storage and database routines to interact with their other services.

Finally at the top layer, software as a service providers inclue: Google Apps (Docs, Groups, Gmail, Calendar, etc) [Google11b], Office Web Apps [Office11], and ThoughtWorks Disaster Relief Appeal [Thought11]. Each of these SaaS solutions is a piece of software that a customer interacts with directly through their web browser. The customer needs no special software installed locally. Data is stored remotely so data does not have to be copied when moving to a new computer. Simple applications like the Disaster Relief Appeal that have been written using a PaaS provider can be developed and published quickly. Also, as resource demands increase more computing power can be dedicated to keep the service available.

It is certainly possible to use an IaaS provider to create a PaaS, which in turn can be used to create a SaaS. This is the case with the ThoughtWorks project above: the software application is built on top of the Heroku platform, which was built using Amazon Web Services.

1.2.2 Standards Organizations

At present the organizations that have the most direct effect on cloud computing security are the National Institute of Standards and Technology [NIST11] and the Cloud Security Alliance [CSA11]. The National Institute of Standards and Technology (NIST) is a government agency that provides national standards so consumers can have a common frame of reference when dealing with new technologies. Specifically, NIST has a cloud computing program designed to “foster cloud computing systems and practices that support interoperability, portability, and security requirements.” [NIST11] The Cloud Security Alliance (CSA) is an organization formed by businesses with an interest in cloud computing security. The primary goal of the CSA is “to promote the use of best practices for providing security assurances within Cloud Computing.” [CSA11] As with NIST, the CSA is seeking to build a common level of security service and assurance for certified cloud providers so consumers know what they are getting.

Since many organizations use cloud computing to provide their services, various standards compliance groups must now enforce and audit the services within a cloud setting. The most notable of these compliance organizations and standards are:

- Payment Card Industry (PCI) Data Security Standard (DSS) certification means some providers can be used for merchant accounts accepting credit card. [PCI-DSS11]
- Federal Information Security Management Act (FISMA) accreditation means the cloud provider can be used and complies with the regulations federal agencies must follow for data security. [FISMA]
- Health Insurance Portability and Accountability Act (HIPAA) does not mandate specific requirements for the cloud provider to obey. However, the requirements do mandate that customers ensure that the provider has and follows certain policies. [HIPAA]

Though these standards do not have a direct effect on what the cloud provider offers other customers, the standards do provide a level of assurance to customers because of what the certification entails. Each of these certifications indicates not that information remains confidential, rather the provider has passed audits using the strict specifications of the certification authority. The cloud customer must work with and understand the constraints and services the cloud provider is responsible for and what the customer must handle.

2 Historical Perspectives

Security is an iterative process that builds on past knowledge to protect against future attacks. Thus, knowing what has happened in the past can be useful when evaluating a new cloud provider or setting up a cloud initially. This section picks some interesting cases of broken security and trust from cloud providers to demonstrate the necessity of cloud security protocols. It is not intended to frighten the reader from using cloud services, but rather highlight the subtle issues involved with cloud security.

2.1 Amazon Web Services meets Spamhaus

In June 2008 there was an malicious email (spam) campaign designed to convince the mail recipients to download an “update” for their computer that was actually creating a back door into the computer. [Krebs08] Unlike typical spam, the emails did not originate from “bulletproof hosting” (a hosting service that refuses to take down malicious users) or a botnet (a network of residential computers that have back doors that allow malicious behavior). Instead it came from a trusted organization—Amazon Web Services.

This is significant because for the first time instead of spam originating from a known bad set of hosts or residential hosts it came from a well-known, legitimate service provider. Since Amazon provides compute instances with dynamic IP addresses the only option for a third party service that tracks offending addresses (known as a spam blacklist provider) was to mark the entire Amazon IP address range as spammers. Any email provider that uses a spam blacklist as input to their mail filtering routines then marks both malicious and legitimate email from Amazon as spam (including purchase receipts, billing statements, marketing campaigns, etc.). This created both a denial of service for honest users and allowed dishonest users to send some number of emails to help build a botnet. It is unfortunately an unavoidable situation when computing is offered at competitive prices (i.e. purchasing time on an Amazon service is comparable or cheaper than purchasing time on a botnet or with a bulletproof host).

Amazon has solved the spam problem by only allowing a limited number of emails from originating within their compute services and offers a separate bulk email service for legitimate users. This protective step allowed Amazon to be removed for the Spamhaus blacklist and allows them to quickly and accurately prevent future abuse. However this problem highlights a preventable issue with cloud providers placing trust in their users to not exploit the system and initially not taking precautions to prevent such an incident from happening.

2.2 Internal Breaches

Not all security problems originate from an external source, sometimes there is an internal breach. For a cloud provider to give reliable service they must be able to effectively diagnose problems when they occur. This means employees of the provider may need to access information that exists in their infrastructure but belongs to a customer. In a typical data center, this necessary access is acceptable because the employees belong to the same organization and are governed by a similar contract. In the cloud setting such a relationship does not exist.

This type of breach happened in mid-2010 when a Google employee with access to email, chat, and phone records abused his position to spy on some users. [Chen10] While typical employees are not given access to such data, some employees need sufficient access to debug problems that occur in running large systems. This employee fell into the group of trusted engineers. Though there were processes in place to monitor employee access to data, the frequency in which they need to access it is great enough that it could not be adequately watched. Once notified of the violation of privacy, Google began an internal investigation, fired the employee, and began more closely watching accesses to customer data. [Chen10]

This instance highlights a potential problem where a customer should be aware that their data is not necessarily protected in the same way it would be if it was kept on the local network. However, if this type of security breach is a risk it is possible to take precautions, such as encrypting data before sending it to the cloud.

2.3 Configuration Errors

One benefit of cloud services is that they can be updated easily and transparently without forcing customers to jump through any hoops. However, this leaves a hole for accidents to go unnoticed which can have significant impact on customers.

In late 2010, Microsoft's Business Productivity Online Suite had a misconfiguration in the deployed version that allowed any user to download another user's address book. [UdodeHaes10] While the error was only live for about two hours, there were still illegitimate downloads from the service. More recently, online storage provider Dropbox deployed a change to their service that resulted in anyone being able to log in as any user without a valid password. [Ferdowsi11] This authentication bug was live for four hours before it was corrected and about 1% of their users were affected in some way.

While reading each of these historical instances of breaches in cloud security it is possible to come to the conclusion that cloud computing inherently means lack of information security. However, even if these were private clouds or non-clouds several of these issues may still arise and go unnoticed for a longer time. By recognizing and facing these issues directly, it is possible to take explicit steps (such as building in application resilience or encrypting confidential data) to prevent or mitigate intrusions or service disasters.

3 Security and Trust

Knowing that there are possibilities for security and trust issues on both sides of the cloud customer-provider relationship allows us to separate what each side should do to build a secure system. This is a paradigm shift from a traditional model where software and computing resources were both provided in-house. While in the internal model, system and network security was mostly handled by the system and network engineers, so even an insecure piece of software would only be accessible to people within the company and particularly offensive software could be removed with ease. In the cloud model, the network engineers are not concerned with these problems and it is up to the cloud customer to protect their data.

3.1 Layers and Obligations for Cloud Security

The broadness of cloud computing and the ramifications of security in the cloud make this a difficult problem to discuss with generalizations because each service provider-customer pair may have different contractual obligations.

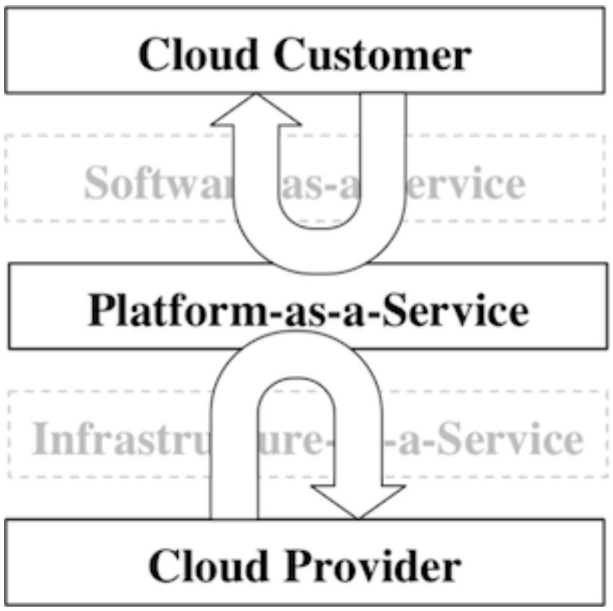

Figure 2: Example of the separation of security concerns between a PaaS customer and provider. Note that there is some overlap where the two meet.

Take Figure 2 as an example. Here the provider is providing the platform as a service to the customer. The customer is responsible for writing software that runs on top of the platform and for ensuring the security of data up to the point it is given to the platform service. This should include encrypting the data if the cloud provider does not do a satisfactory job of protecting the data (i.e. using a weak cipher, the details of which *should* be disclosed when signing up for the service). The provider is responsible for securing the infrastructure (network connectivity, physical machines, and platform environment). When the underlying provider services meet the customer software implementation there should be a clear, well defined interface for transferring data from customer to provider. [NIST500-292]

```
def EncryptAndStoreObject(name, data) :
    """
    Encrypt and store an object consisting of `data` with the identifier
    `name`.  This method encrypts the `data` object using AES-256 with the
    unique key associated with your account (available from your account
    settings page). The identifier `name` is not encrypted, but it is not
    available to other accounts, only our system engineers.
    """
    # implementation
```

Figure 3: Code snippet with a well-defined interface between the cloud customer and cloud provider.

For example, a platform provider may include an interface for storing files to their storage infrastructure which can be seen in Figure 3. The customer would read the documentation and recognize that the provider does encrypt the data that is stored to their storage platform, however it is done with a key that the provider knows. This method would therefore protect your data from external threats and unauthorized internal threats, but remain open to *authorized* internal threats (such as the one described in Section 2.2 with a Google employee accessing private data). There is also a threat that some outside force may discover the platform provider's key generation routine or the key itself. These threat may be an acceptable risk to the customer,

allowing them to use the storage routine without providing their own security. If these risks are not acceptable, the customer can provide their own wrapper method that encrypts the data using their own key prior to using the platform's storage function.

There should be similar separations at the SaaS and IaaS levels. It is in the purview of the SaaS provider to decide how the data should be stored. For example, it is the decision of Gmail to store your emails on their servers as an encrypted byte stream or in plain text. This prevents unauthorized people from accessing the emails, but since the key used for encryption is in their possession, anyone with sufficient access can view the message. The customer of a SaaS provider is somewhat limited in security terms, but their obligations include using a secure web browser, a secure operating system, and ensuring the connection is done using SSL.

On the other end, an IaaS provider must ensure that their network and physical machine are secure while the customer is responsible for operating system, runtime, and application security. In the case of Amazon Web Services, the provider is responsible for keeping their physical resources secure and available, while still allowing their customers to run whatever operating system they choose and preventing two customers from conflicting with one another. It then becomes the responsibility of the cloud customer to install an operating system (typically the IaaS provider also has some default options), configure the services and interactions, and secure anything the customer deems necessary.

3.2 Ownership Issues

As with above, ownership is a contractual issue. Ownership rights can vary between providers, however there are certain items that should be considered (such has what party owns the copyright and who can use or sell the data). [McDonald10] Whenever software or data assets are sent from a customer to a cloud provider there is an opportunity for the cloud provider to take or use that data. This is most prevalent by SaaS providers because they can extract value from the data.

The prime example of this is Gmail's advertisements. While you are the owner of the content of emails sent using Gmail, Google uses its algorithms to parse the email to deliver advertisements that may be of interest to you based on the email itself. [Google11d] Employees do not read your email, however computers that Google owns do process your email to provide relevant advertisements.

3.3 Attack Possibilities

Attacks are an interesting problem with cloud services. While operating in the cloud can make a customer's job easier with respect to security considerations (as the cloud provider bears some of that burden), it also opens new attack vectors that complicate matters.

3.3.1 Service Provider Attack

Assume you have built an application with zero security holes and are using a PaaS provider to host your application. Your application depends on parts of their platform to be useful. These dependencies may directly include storage, database, a web server, and a code interpreter. Additionally you depend on their servers, network, and deployment infrastructure. If attackers are targeting any of your providers systems, it in turn makes your application vulnerable to attack. The most common scenario would be a denial of service attack that makes communication with your application impossible because the provider's network has been overloaded. It is also possible that their physical systems are cracked and data storage systems compromised. Depending on the precautions the provider has taken, your data may now be compromised.

3.3.2 Side-Channel Attack

There is also a certain amount of trust put in other applications that may be running on the same physical system as yours. Attacks of this variety of typically referred to as "side-channel" attacks because the attack is able to succeed through indirect means instead of direct exploitation. [Ristenpart09]

This style of attack is enabled because most cloud providers use virtual machines to safely separate two customers from one another at a logical (not necessarily physical) level. If an attacker can manage to get one of their virtual machines assigned to the same physical host as the victim they may be able to break out of their sandbox or consume and unfair share of resources. This resource exhaustion would lead the victim system to become unresponsive or unavailable. In the worst case, the attacker may be able to use low-level exploits to infect the physical machine an snoop their victim's traffic.

3.3.3 Distributed Denial of Service

A third attack vector is being an indirect victim of a denial of service attack. As mentioned above, a cloud provider likely uses virtual machines that run on physical hosts which means shared resources. These resources include networking systems which can be overloaded in certain situations. As such, if a one customer is the target of an attack it is possible that an unrelated customer is adversely affected by the same attack. For example, assume Amazon Web Services hosts both a controversial web site and a social news aggregator. Now a large group of people want to take down the controversial web site. To do this each member of the group continuously sends requests until the web site can longer fulfill the requests; the controversial web site is now unavailable. However, since the social news aggregator was hosted using the same physical resources it is also a victim of the attack. Providers can mitigate this style of attack by distributing resources fairly and customers can use multiple physical locations to ensure availability.

Though it is the responsibility of the cloud provider to protect against these attack vectors, the customer must be aware of the potential and take steps to provide assurances that their service are not be adversely affected. This can be done by hosting the service with multiple cloud providers (or at multiple locations of the same provider) and protecting your own data instead of relying on the cloud provider to protect the data.

4 Security Offerings and Compliance

So far this paper has simply presented some of the security considerations when using cloud service provider. It is also useful to look at existing cloud providers to see what assurances and compliance they offer. Section 4.4 also looks at recent reports from the CSA's working group on security as a service (SecaaS).

4.1 Google Apps

Google Apps includes several SaaS solutions including Gmail, Google Calendar, and Google Docs. [Google11c] These services are frequently used by businesses instead of their own in-house versions because it is lower cost to use an external service provider. As such, Google Apps must explain how they secure their service offerings. Like most cloud providers, Google Apps has completed a Statement on Auditing Standards Number 70, Type II (SAS 70, Type II). SAS 70, Type II is a standard auditing system that provides potential cloud customers a consistent method to review procedures (including security procedures) that a cloud provider has in place. Additionally, Google Apps has passed FISMA certification meaning that they are compliant with federal law for holding data for government agencies.

Beyond the certifications, Google also employs several security procedures to ensure the protection of data. Google Apps allows two-factor authentication so users must provide their password and a token identifier sent to their mobile phone or generated on a pocket device. Access to their services is HTTPS enabled so data can be protected in transit. Host systems are custom built with security in mind to reduce the attack surface of

the installed system. Data stored on Google's servers is replicated to several data centers so even a major outage to a data center does not destroy the data. Google also performs internal audits of their application code, as well as having external audits. Physical access to data centers is restricted to an as-needed basis and the data centers themselves have network and power redundancies. While these precautions do not affect the confidentiality of data, they can help ensure both the integrity and availability of data.

4.2 Windows Azure Platform

The Windows Azure system is a PaaS provider that includes three core components: compute, storage, and service management. [Kaufman10] These services allow developers to use the .NET framework, SQL Azure, and Azure Storage to create web applications hosted using Microsoft data centers around the world. As with Google Apps, Windows Azure has completed a SAS 70, Type II audit and has FISMA certification. Unlike Google Apps, Windows Azure has also completed ISO 27001 certification. ISO 27001 certification is similar to SAS 70, Type II in that it provides a consistent report to customers to evaluate different cloud providers fairly. Unlike a SAS 70, Type II audit, an ISO 27001 audit is focused specifically on security practices instead of a general audit of the procedures in place.

In the actual realm of security, Windows Azure Platform provides several security mechanisms to keep data protected. Customers must authenticate with their Windows Live Identifier so as to correctly identify themselves as an authorized client to help prevent unauthorized access to backend systems. Data stored on the platform is encrypted *within* Windows Azure, so even a breach of their security systems does not make data stored by your application available. Each customer's data is logically separated onto a different (virtual) volume so it is difficult to access another customer's data. As with Google Apps, data can be replicated at several locations so catastrophic failure does not imply data loss; it is also possible to restrict the geographic location of your data to comply with potential import/export regulations that the data may fall under. Again, physical access is restricted to their data centers and redundant network and power systems minimize likelihood of intermittent failures.

4.3 Amazon Web Services

Amazon Web Services (AWS) is an IaaS provider offering a range of services including: Elastic Computer Cloud (EC2), Simple Storage Service (S3), Simple Email Service (SES), and Route 53 (DNS) among others. [Amazon11b] Many companies use AWS because of the build it yourself mentality where they do not have to learn to work in the confines of a PaaS provider but can build their own platform and provide their own security. That said, it is still important for Amazon to certify their systems so customers are comfortable building and hosting software with them. Like Google Apps and Windows Azure, AWS has completed a SAS 70, Type II audit and FISMA requirements. They have also gone through the ISO 27001 certification processes. Unlike Windows Azure they have taken the steps necessary to be PCI-DSS compliant; meaning customers can host a payment system on Amazon servers instead of using a third-party service. This means Amazon has a secure network, card holder data can be protected, vulnerability management programs are in place, monitoring can be done, and security policies are in place. [PCI-DSS11] They have also had clients successfully complete HIPAA certification, meaning AWS can be used as a health information service.

Like Google Apps and Windows Azure, AWS data centers have physical security with limited employee access (which is re-evaluated every 90 days) to both the physical systems and customer data. AWS offers multi-factor authentication to prevent unauthorized users from logging into system controls. Within their network there are several strict policies in place to prevent IP address spoofing from within their data centers and shut down port scanning. Customers that try to use traffic sniffers to spy on other tenants will be unsuccessful because any virtual network interface will be behind a firewall on the host machine to prevent any traffic not destined for that host from arriving. [Amazon11c] Amazon also uses a proprietary system to prevent distributed denial of service (DDoS) attacks from affecting user services. This system has successfully

sustained the load of large web traffic days (like "Black Friday") and targeted DDoS attacks by the "hacktivist" group Anonymous. [Stambor09, Pepitone10]

4.4 Security as a service

Security as a service (SecaaS) is a recent working group under the CSA purposed with developing standards for "the provision of security applications and services via the cloud either to cloud-based infrastructure and software or from the cloud to the customers' on-premise systems." [SecaaS11] The group produced a document defining the categories of most interest to customers that was finalized in September 2011. Those areas of interest are as follows [SecaaS11]:

- Identity and Access Management ensures that only authorized users are able to access their resources.
- Data Loss Prevention ensures that data cannot be removed without authorization.
- Web Security protects customers from downloading malicious content.
- Email Security protects customers from sending or receiving malicious emails.
- Security Assessments would require standards based (ISO, SAS, etc.) auditing of cloud providers.
- Intrusion Management allows the real-time detection and prevention of intrusions.
- Security Information and Event Management is a service that would let customers know of any lapses in security.
- Encryption provides services for protecting data from eavesdroppers.
- Business Continuity and Disaster Recovery provides customers with options or methods for coming back after a worst-case scenario.
- Network Security provides mechanisms that prevent unauthorized access of resources.

Each of the above areas of "of interest" to the SecaaS working group and may not be realized. The end goal of this group is to provide a standard that cloud providers could follow and provide organizations with certain security assurances. For example, if a cloud customer wants to monitor intrusions to their system they could talk to a SecaaS provider and use a cloud monitoring system instead of installing or building their own.

Unfortunately, as of this writing no more documents have been produced by the SecaaS working group, but it should be noted that it was only formed in July 2011 and such standardizations take time.

5 Conclusions

Cloud computing is a ripe field that offers very competitive advantages over the traditional in-house service provider, however there is no magic bullet in the realm of security and cloud computing is no exception. Both the cloud customer and cloud provider must be aware of their respective security obligations. Since cloud computing is a paradigm shift from traditional computing, it is difficult to compare based strictly on one aspect of the system. While traditional computing allows a developer to be more lax about security, a cloud computing environment forces a good developer to face these issues directly. However, cloud computing also opens customers to new attack vectors and possibly indirect attack vectors.

Since the cloud customer is closer to the end-user of the system, it is their responsibility to provide security from the top-down and ensure that the cloud provider takes care to protect the system from the bottom-up and from the side. This paper has taken care to provide the reader with enough information to make informed decisions when looking for a cloud provider and what responsibilities a software developer should take when building a cloud application.

References

Ordered by relative importance to this paper.

1. [NIST500-292] "NIST Cloud Computing Reference Architecture," Special Publication 500-292, September 2011, pages 15—17, http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/ReferenceArchitectureTaxonomy/NIST_SP_500-292_-_090611.pdf. NIST document describing security expectations in a cloud computing environment.
2. [NIST11] "NIST Cloud Computing Program," retrieved November 14, 2011, http://www.nist.gov/itl/cloud/index.cfm. Landing page for the NIST cloud computing program to differentiate the three models of cloud computing.
3. [NIST800-145] Peter Mell and Timothy Grance, "The NIST Definition of Cloud Computing," Special Publication 800-145, September 2011, pages 2—3, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. Short NIST document defining cloud computing models and services.
4. [CSA11] "Cloud Security Alliance," retrieved November 14, 2011, http://www.cloudsecurityalliance.org/. Landing page for the Cloud Security Alliance.
5. [Amazon11c] "Amazon Web Services: Overview of Security Processes," Amazon Web Services, May 2011, http://d36cz9buwru1tt.cloudfront.net/pdf/AWS_Security_Whitepaper.pdf. Presents Amazon Web Services' security policies and procedures for preventing attacks.
6. [Golden11] Bernard Golden, "Cloud CIO: The Two Biggest Lies About Cloud Security," CIO, May 2011, CXO Media, http://www.cio.com/article/print/683075. Discusses two major misconceptions about cloud security.
7. [Krebs08] Brian Krebs, "Amazon: Hey Spammers, Get Off My Cloud!" The Washington Post, July 1, 2008, http://blog.washingtonpost.com/securityfix/2008/07/amazon_hey_spammers_get_off_my.html. Explains the nature of Amazon IP addresses being blacklisted by Spamhaus and other organizations.
8. [Chen10] Adrian Chen, "GCreep: Google Engineer Stalked Teens, Spied on Chats," Gawker Media, September 14, 2010, http://gawker.com/5637234/gcreep-google-engineer-stalked-teens-spied-on-chats. Explains the nature of a rouge Google employee violating the privacy of customers.
9. [Ferdowsi11] Arash Ferdowsi, "Dropbox: Yesterdayâ€™s Authentication Bug," Dropbox Blog, June 20, 2011, http://blog.dropbox.com/?p=821. Explains what happened and the steps to prevent the Dropbox authentication bug allowing anyone access to files.
10. [UdodeHaes10] Andreas Udo de Haes, "Microsoft BPOS cloud service hit with data breach," Computerworld Inc., December 22, 2010, http://www.computerworld.com/s/article/9202078/Microsoft_BPOS_cloud_service_hit_with_data_breach. Explains the breach of one Microsoft cloud service and the effect it had.
11. [McDonald10] Steve McDonald, "Legal and Quasi-Legal Issues in Cloud Computing Contracts," EDUCAUSE and NACUBO Workshop on Cloud Computing and Shared Services, February 2010, http://net.educause.edu/section_params/conf/CCW10/issues.pdf. Provides examples of items that should be covered in any contract with a cloud provider (in the higher education setting).
12. [Amazon11b] "AWS Security and Compliance Center," retrieved November 14, 2011,http://aws.amazon.com/security/. Describes Amazon Web Services' security certifications and features to protect your data.
13. [Google11c] "Google Apps for Business: Security First," retrieved November 14, 2011, http://www.google.com/apps/intl/en/business/infrastructure_security.html. Describes from a high-level the security of Google Apps for Business SaaS solution.
14. [Kaufman10] Charlie Kaufman and Ramanathan Venkatapathy, "Windows Azure Security Overview," Microsoft, version 1.01, August 2010, http://go.microsoft.com/?linkid=9740388. Describes how the Windows Azure Platform approaches security.
15. [SecaaS11] "Security as a Service (SecaaS)," retrieved November 14, 2011, https://cloudsecurityalliance.org/research/working-groups/secaas/. Landing page for the SecaaS working group of the CSA.
16. [Ristenpart09] Thomas Ristenpart, Eran Tromer, Hovav Shacham, and Stefan Savage, "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Part Compute Clouds," ACM Conference

on Computer and Communications Security, November 2009, Chicago, IL, http://cseweb.ucsd.edu/~hovav/dist/cloudsec.pdf. Describes potential side channel attacks on cloud users.
17. [Pepitone10] Julianne Pepitone, "Why attackers can't take down Amazon.com," CNN Money, December 9, 2010, http://money.cnn.com/2010/12/09/technology/amazon_wikileaks_attack/index.htm. Describes "hacktivist" group Anonymous' failed attempt to take down Amazon.
18. [Stambor09] Zak Stambor, "Amazon leads Black Friday web traffic; Walmart was tops on Thanksgiving," Internet Retailer, November 30, 2009, http://www.internetretailer.com/2009/11/30/amazon-leads-black-friday-web-traffic-walmart-was-tops-on-thank. Demonstrates Amazon's ability to handle large influxes of distributed traffic that isn't designed to take down a service provider.
19. [Amazon11a] "Amazon Elastic Compute Cloud (Amazon EC2)," retrieved November 14, 2011, http://aws.amazon.com/ec2/. Highlights several service facts about Amazon's EC2 systems.
20. [Rackspace11] "The Rackspace Cloud," retrieved November 14, 2011, http://www.rackspace.com/cloud/. Describes the services provided by the Rackspace Cloud.
21. [IBM11] "IBM SmartCloud Infrastructure as a Service," retrieved November 14, 2011, http://www.ibm.com/cloud-computing/us/en/iaas.html. Discusses IBM's role in providing cloud services using their systems.
22. [Google11a] "Google App Engine," retrieved November 14, 2011, http://code.google.com/appengine/. Presents the platform interfaces used when building web applications on Google's PaaS solution.
23. [Heroku11] "Heroku Cloud Application Platform," retrieved November 14, 2011, http://www.heroku.com/. Entry point for using the Heroku PaaS for building web applications.
24. [Azure11] "Windows Azure Platform," retrieved November 14, 2011, http://www.microsoft.com/windowsazure/. Entry point for using the Windows Azure Platform for building web applications.
25. [Google11b] "Google Apps for Business," retrieved November 14, 2011, http://www.google.com/apps/intl/en/business/index.html. Describes Google Apps that are used by businesses and links to security white papers regarding their services.
26. [Office11] "Office Web Apps," retrieved November 14, 2011, http://office.microsoft.com/en-us/web-apps/. Describes Microsoft's Office Web Apps SaaS for businesses.
27. [Thought11] "ThoughtWorks Success Story," retrieved November 14, 2011, http://success.heroku.com/thoughtworks-flood. Describes the speed and security of a disaster relief web application built on Heroku.
28. [SeWHiP] "Southeast Wisconsin High Performance Computing," retrieved November 26, 2011, http://www.sewhip.org/. Explanation of the communal cyberinfrastructure in place for southeastern Wisconsin.
29. [PCI-DSS11] "PCI SSC Data Security Standards Overview," retrieved November 14, 2011, https://www.pcisecuritystandards.org/security_standards/. Landing page describing what the PCI-DSS standard is and does.
30. [FISMA] "Federal Information Security Management Act (FISMA) Implementation Project," retrieved November 14, 2011, http://csrc.nist.gov/groups/SMA/fisma/index.html. Landing page for NIST's guidelines for being a FISMA compliant provider.
31. [HIPAA] "Health Information Privacy," retrieved November 14, 2011, http://www.hhs.gov/ocr/privacy/. Landing page for describing what the HIPAA is and how it bears on cloud computing.
32. [Google11d] "Ads in Gmail and your personal data," retrieved November 15, 2011, https://mail.google.com/support/bin/answer.py?answer=6603. Description of how Google servers use machine learning to provide relevant advertisements in the web interface.

List of Acronyms

AWS	Amazon Web Services
CSA	Cloud Security Alliance
DDoS	Distributed Denial of Service

DNS	Domain Name System
EC2	Amazon Elastic Compute Cloud
FISMA	Federal Information Security Management Act of 2002
GAE	Google App Engine
HIPAA	Health Insurance Portability and Accountability Act
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure as a Service
IBM	International Business Machines
IP	Internet Protocol
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
PaaS	Platform as a Service
PCI-DSS	Payment Card Industry-Data Security Standard
S3	Amazon Simple Storage Service
SaaS	Software as a Service
SAS	Statement on Auditing Standards
SecaaS	Security as a Service
SES	Amazon Simple Email Service
SSL	Secure Sockets Layer
SQL	Structured Query Language

Last modified on November 16, 2011
This and other papers on latest advances in network security are available on line at
http://www1.cse.wustl.edu/~jain/cse571-11/index.html
Back to Raj Jain's Home Page