(In)Security above the Clouds

Javier Echaiz Jorge Ardenghi

Laboratorio de Investigación de Sistemas Distribuidos (LISiDi)
Departamento de Ciencias e Ingeniería de la Computación
Phone: +54 291 4595135, Fax: +54 291 4595136
Universidad Nacional del Sur, Bahía Blanca (8000), Argentina
{je,jra}@cs.uns.edu.ar

Abstract

In an ideal world, organizations "share" the cloud, logically separated from each other by the cloud provider, operating independently of each other in a sandbox, pulling resources only when needed, and respecting the separation put in place by the cloud provider. In the real world, applications uploaded to the cloud are trying to break out of their sandbox, attempting to gain access to other applications and hardware and trying to consume resources. The attackers know they have complete control of what the cloud runs; they know cloud security is immature and developing.
Cloud computing creates new security problems that must be dealt with in addition to the existing problems.
This research line explores these security problems.
Keywords: cloud computing, security, SaaS, PaaS, IaaS.

Context

This research line is part of the following research projects:

- High Performance and High Availability Distributed Computing (Spanish: Computación Distribuida de Alto Rendimiento y Disponibilidad). Code: 24/N024. Secretaría de Ciencia y Tecnología, Universidad Nacional del Sur, Bahía Blanca, Argentina (2008-2010). Project coordinator: Jorge R. Ardenghi.
- Automatización de la Detección de Intrusos a partir te Políticas de Seguridad. Code: 24/ZN14. Secretaría de Ciencia y Tecnología, Universidad Nacional del Sur, Bahía Blanca, Argentina (2008-2010). Project coordinator: Javier Echaiz.

1. Introduction

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential **characteristics,** three **service models**, and four **deployment models**.

Essential Cloud Characteristics

On-demand self-service. *A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.*

Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).

Resource pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

Rapid elasticity. Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

Measured Service*.* Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

Service Models

Cloud Software as a Service (SaaS). The capability provided to the consumer is to use the 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 (e.g., web-based email). 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.

Cloud Platform as a Service (PaaS)**.** The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications 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.

Cloud Infrastructure as a Service (IaaS). The capability provided to the consumer is to 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 (e.g., host firewalls).

Deployment Models

Private cloud. The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.
Community cloud. The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.
Public cloud. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
***Hybrid cloud*.** The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

Cloud software takes full advantage of the cloud paradigm by being service oriented with a focus on statelessness, low coupling, modularity, and semantic interoperability.
Next section summarizes the main security issues, once again we can see "there ain't no such thing as a free lunch".

2. Main Cloud Security Issues

#1: All the Eggs in One Basket
Moving data to a cloud service is the equivalent of "putting all the eggs in one basket". Not too long ago, we saw a perfect example of the worst-case scenario of doing just that. In 2009 social bookmarking site Ma.gnolia experienced a server crash that resulted in massive data loss , enough to shut down the service for good. Users' bookmarks were lost forever.

While that incident may have had only a minimal impact on the world at large, there are other examples that were much worse, including that of online storage service MediaMax (also called The Linkup) which went out of business following a system administration error that deleted active customer data. Then there was the incident where Salesforce.com customers were locked out of their critical business applications during a service outage. Finally, we saw the Nokia's Ovi crash which resulted in three weeks of lost user data as contacts simply disappeared from people's phones. There were no backups in place, either.
These incidents highlight some of the pitfalls that can come from trusting cloud services, and it's precisely for those reasons that enterprise IT is making the move at a much slower rate than consumers. This is especially true in heavily regulated industries where compliance is an issue.

#2: Too Much Trust?

If you want to set up a new instance on Amazon's Elastic Compute Cloud (EC2) the first step is to create a new Amazon Machine Image (AMI) containing your applications, libraries, data, and other associated configuration settings. However, as an alternative, you could use a pre-configured templated image to get up and running quickly. There's only one problem with that, though. While Amazon has provided 47 machine images they built themselves, the remaining thousands images were build by other EC2 users. Can you really believe that all of these images were built securely? Basically, the

template directory is just a big archive of user (risky) generated content.

#3: Reliance on Passwords

Another issue with cloud computing services is that, despite the numerous protections built into a cloud service itself, any account is only as secure as the password used to access it. A recent example of the consequences of insecure passwords was seen during what has now become known as "Twittergate." The microblogging service Twitter had their online accounts accessed by a hacker and numerous sensitive corporate documents stolen. The documents were housed in Google's online web office service Google Docs. Although Google was not to blame for the break-in, the hack may not have ever occurred in the first place if documents were securely hosted on-site, behind a firewall. Instead, the entire company data was only one password crack away from discovery.
Password cracking is not the only threat from what is seemingly becoming a more and more archaic system for logging into online services. Weak password recovery systems are an issue, too. Password resetting and other security mechanisms in the cloud are always going to be a weak link, as long as user-friendliness comes ahead of security in the cloud computing beauty stakes. Expecting regular joes to whip out a two-factor authentication device for use with a cloud-driven service just isn't realistic.
But without more secure methods of gaining access to cloud services, users themselves are the weakest link. Of course, this issue is not new. IT administrators have struggled with users' lack of good security practices for years (in fact since computers required a password). However, the difference between a corporate network and an online account is that in a business environment, administrators can create server-enforced password policies that require users to make up passwords with certain minimum levels of complexity. They can also force users to reset their passwords on a regular basis. But in the cloud, a user could set their password to "123456" and never change it again.

Some cloud vendors are beginning to offer security policy control for their applications which would allow an IT admin to create and enforce stricter policies (like a secure password policy, for instance). Today, though, this is an area where many cloud applications are still lacking.

#4: Encrypting Data in the Cloud

Many cloud providers do not offer encryption for their service. For example virtual machines don't always have enough access to the random numbers needed to properly encrypt data. The end result is that the very nature of virtual computing itself makes hacking simpler because it allows attackers to more easily guess the numbers used to generate the encryption keys.
Of course this problem isn't an immediate threat to cloud computing, but it does require more research.

3. Conclusions

Is the cloud really all that bad? Is it any worse of a platform for computing than what we had before? Probably not. Although the cloud will provide a new set of challenges and threats to deal with - and these will be more prevalent in the early stages of the transition - it doesn't necessarily present threats that are that

dramatically worse than old-school on-site computing.
In the end, some cloud vendors will step up and make their cloud applications more secure, layering in security policies, encryption and the like while doing their best to mitigate the single-point-of-failure issues. Those vendors will eventually be rewarded for their efforts as more users, and then businesses, adopt their platform. Those that ignore the security issues will soon fall out of favor.
Today's cloud services may not be as secure as they should be, but in time they could easily rival any other computing platform. in fact, they may one day be considered more secure. Until then, though, users, and especially companies, should proceed with caution when moving to the cloud, making sure they're fully aware of not only the capabilities of the online service, but the risks as well.

4. Research Line

Considering the above issues it is clear cloud security is still immature.
We are just starting a research line that integrates identity and access management in cloud computing in order to extend corporate security policies to this new computing paradigm.
The idea is to improve the cloud infrastructure using industry standards and combining security policies and training programs, since the human factor is still the main security problem.

References

1. F. John Krautheim, *Private Virtual Infrastructure for Cloud Computing*, 2009.
2. Robert L. Grossman, *Cloud Computing: The Case for Cloud Computing*, 2009.
3. Nuno Santos, Krishna P. Gummadi, and Rodrigo Rodrigues. *Towards Trusted Cloud Computing*. HOTCLOUD, 2009, USENIX.
4. Christian Cachin, Idit K. Alex, and Er Shraer. *Trusting the Cloud*, 2009.
5. John Rittinghouse, and James Ransome. *Cloud Computing: Implementation, Management, and Security*. 2009, CRC Press.
6. Tim Mather, Subra Kumaraswamy, and Shahed Latif . *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*. 2009, O'Reilly.
7. George Reese. *Cloud Application Architectures: Building Applications and Infrastructure in the Cloud*. 2009, O'Reilly.
8. Jeff Barr. *Host Your Web Site On The Cloud: Amazon Web Services Made Easy: Amazon EC2 Made Easy.* 2010, SitePoint.
9. Scott Granneman. *Google Apps Deciphered: Compute in the Cloud to Streamline Your Desktop*. 2008, Prentice Hall.
10. Dimitris N. Chorafas. *Cloud Computing Strategies*. 2010, CRC Press.
11. Toby Velte, Anthony Velte, and Robert Elsenpeter. *Cloud Computing, A Practical Approach*. 2009, McGraw-Hill.
12. Peter Fingar. *Dot Cloud: The 21st Century Business Platform Built on Cloud Computing*. 2009, Meghan-Kiffer Press.
13. Marc Benioff, and Carlye Adler. *Behind the Cloud: The Untold Story of How Salesforce.com Went from Idea to Billion-Dollar Company-and Revolutionized an Industry*. 2009, Jossey-Bass.
14. John Rhoton. *Cloud Computing Explained: Implementation Handbook for Enterprises.* 2009, Recursive Press.