Securing the Cloud Infrastructure

Zachary Sogard

12/15/15

Abstract

As organizations experience rapid growth in data storage requirements, information technology teams are pressured to make their data storage operations more efficient in terms of cost and resources. Cloud computing offers a much more efficient means of setting up and maintaining the infrastructure required to meet these high demands for cheap data storage. However, cloud computing presents an increased potential for vulnerabilities and thus, a variety of new security challenges. This paper will examine a few of the major concerns cloud computing creates such as increased spread of attack and multiple clients using the same infrastructure. Then, I will explore the security methods currently employed in data centers today. This will detail a comprehensive defense-in-depth approach to security from the software level down to the platform and infrastructure level. Finally, the paper will take a brief look at the future of security in the cloud.

Introduction and Background

In a traditional private data center, an enterprise that requires networking and computing resources would have to invest a considerable amount of capital into the infrastructure, software, and management of these resources with little to spare for development of the enterprise's core products. Cloud computing is becoming widely

adopted as a solution to this problem by providing cheap computing resources and represents a large shift in information technology.

However, to understand the increased concerns for security in a cloud computing environment, business decision makers first need to understand what we exactly mean by cloud computing and its different forms of services and deployment. The National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling ubiquitous, 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 is composed of five essential characteristics, three service models, and four deployment models." [4] The five essential characteristics are on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.

On-demand self-service is defined as the ability for a customer to easily and quickly provision computing resources that it needs via an online portal rather than contacting humans working for the provider. Broad network access defines the ability for end users to access the hosted application on a variety of different devices ranging from laptops to workstations. Resource pooling says that the cloud service provider (CSP) must supply resources in a multi-tenant model where several customers share resources

while the CSP maintains appropriate mappings between the physical infrastructure and each individual customer's virtual environment. Rapid elasticity guarantees that customers can easily scale-up or scale-down the amount of desired resources easily. Finally, measured service requires that the CSP automatically monitor the usage of resources by each customer to be charged similar to how a home utilities bill is generated.

Additionally, there are several types of services these CSPs can provide: infrastructure, platform, and software. Infrastructure as a Service (IaaS) is a cloud service model in which the CSP provides the bare networking, compute, and storage components required for the cloud-enabled applications. The customer then installs its own operating system (OS), file system, environment, and applications on this infrastructure. Platform as a Service (PaaS) describes a model in which the CSP provides services such as the operating system, development and runtime environment, and web servers in addition to the infrastructure. Finally, Software as a Service (SaaS) defines a service in which the CSP provides everything required from the infrastructure and platform services as well as the specific application that the customer desires. While IaaS provides customers with the most flexibility in services, SaaS gives customers much more simplicity since the customer does not need to concern itself with the underlying setup and management of the infrastructure.

Furthermore, there are four main types of cloud deployment models: private, community, public, and hybrid. Private cloud describes a single organization consisting of multiple business units collectively sharing its resources. Community cloud describes a set of organizations with similar goals and compliance considerations sharing cloud resources. Public cloud describes cloud resources available for general use by anyone. Finally, hybrid cloud is a deployment of any combination of these resources. For example, a business may want full control over its mission critical application, so it will use private cloud for it, but it will use public cloud for less essential applications. Again, there is a trade-off in flexibility versus simplicity as we go from private to public cloud.

To the Community

As explained above, cloud computing presents a seemingly easy solution to saving organizations' money. According to the Cloud Security Alliance, this exciting technology provides customers with “opportunities to reduce capital costs” and “divest themselves of infrastructure management, and focus on core competencies.” [5] Consequently, companies have followed suit by moving a vast amount of data to the cloud. However, cloud computing comes with its own security risks that are either not present or not as severe in a traditional data center setting. Furthermore, companies that favor simplicity and adopt public deployment or SaaS have less control over where and how their data is stored as well as the implementation of the management and security measures to

protect it.

CSPs must be aware of the concerns enumerated in this paper to ensure the risk triad security goals of confidentiality, integrity, and availability as well as accountability are met and how they are more difficult to achieve with cloud computing. Since cloud computing includes multi-tenancy of resources, it becomes more difficult to ensure confidentiality and integrity of data because there is the increased risk of one customer's environment being able to unintentionally view or modify another's. Furthermore, if one customer's environment is compromised, it is much easier for an attacker to consequently gain access to other customers' environments within the cloud. In other words, cloud computing presents the potential for very high velocity of attack. Srinivasan et al., states that "providing security to the user data, which is logically segregated, from any other user (and/or CSP) in terms of unauthorized access/attacks, isolation of data, and maintaining proper compliance & SLAs becomes the order-of-the-day of all cloud computing security concerns." [3]

Additionally, availability becomes an increased challenge when the cloud must guarantee rapid elasticity. If a customer desires to greatly scale-up its desired resources, the CSP must be able to allocate the required infrastructure necessary to maintain availability of data. Bisong and Rahman of Capella University paint this issue in a real-world situation: "Imagine an enterprise that completely depends on a cloud computing

service provider whose system had been disrupted for hours or days. The loss of business could be catastrophic." [1]

Finally, a focus on accountability is necessary to distinguish events and operations on each customer's individualized virtual environment so that these can be properly audited and traced. Leaders in IT and business decision makers must be aware of these heightened risks when utilizing cloud computing for their applications and need to factor in the concerns of data confidentiality, integrity, availability, and accountability when making these decisions.

Action Items

There is a large attack surface within the cloud computing environment that attackers can attempt to exploit. According to EMC Corporation, there are three major domains in which these attacks can occur: application, management, and backup and replication. [2] Some common threats include spoofing user identity, elevating privileges, tampering with data at rest and in flight, network snooping, denial of service (DoS), and media theft. In the management domain, attackers can potentially spoof identity to be an administrator, elevate administrative privileges, or perform network snooping and DoS. Finally, backup and replication can be attacked by spoofing the identity of the backup site so that the data is sent elsewhere, tampering with data in flight and at rest, and network snooping. Since there is such a large variety of attacks that can be

performed on the cloud, CSPs must provide a defense in breadth and in depth to prevent the success of these attacks and achieve the goals of confidentiality, integrity, availability, and accountability.

The beginning of any good cloud defense begins with protecting the infrastructure itself. To secure the network components, a variety of measures that should be taken to ensure limited visibility and access between tenants. For example, Vic Winkler from Microsoft Technet Magazine states that "one actual practice for managing traffic flows between VMs is to use virtual local area networks (VLANs) to isolate traffic between one customer's VMs from another customer's VMs." [6] Similarly, a common fiber optic protocol used in data centers called Fibre Channel allows the network to be split into multiple zones. Communication cannot travel across zones. This partitions the network into multiple sections to limit access across tenants. Finally, data-in-flight encryption can be employed to prevent network snooping. All of these measures limit the spread and velocity of attack as well as inhibit attackers from gaining access to resources via the network infrastructure.

Network authentication can be implemented using a protocol such as Kerberos or the Challenge-Handshake Authentication Protocol (CHAP). Kerberos requires clients to obtain proper authentication before establishing sessions with servers. The client must first contact the Kerberos server to obtain a limited validity ticket which it can then use

to establish encrypted communication with the desired server. The Kerberos server only grants this if it finds that the client is listed within its Active Directory. CHAP is a different authentication protocol in which the client shares a secret with the node it wants to connect to. When the client contacts the target, the target responds with a "challenge". The client computes the MD5 hash of the secret and sends it back to the target. The target computes its own MD5 hash and compares it with the value it received. If they matched, authentication is acknowledged. More information about Kerberos and CHAP can be found in the supporting video.

There are also a couple of measures that can be taken to secure the storage arrays in a data center. For example, Logical Unit (LUN) masking is a common technique that EMC recommends. [2] A LUN is a storage resource that resides on a storage array and is accessed by servers. LUN masking entails configuring the network such that certain servers can only see the LUNs they are meant to see and no others. Additionally, data-at-rest encryption should be used on the data resident in the array. By doing so, any attacker who still happens to gain unauthorized access to the data on the storage array will not be able to make use of any of it. This ensures data integrity and confidentiality.

The last component of infrastructure to secure is the server. The server consists of the hypervisor which controls several virtual machines (VMs), each with their own

OS. According to Winkler, "one potential new risk has to do with the potential to compromise a virtual machine (VM) hypervisor. If the hypervisor is vulnerable to exploit, it will become a primary target. At the scale of the cloud, such a risk would have broad impact if not otherwise mitigated. This requires an additional degree of network isolation and enhanced detection by security monitoring." [6] Consequently, it is especially critical that any security-related updates are installed on the hypervisor as frequently as possible. Also, the hypervisor management system should have a dedicated firewall to ensure only authorized administrators can configure it. Additionally, VM isolation or hardening is essential. This is a setting implemented at the hypervisor level that isolates the execution environment of each VM. Therefore, if one VM becomes compromised, the spread of attack is limited to the compromised VM.

CSPs need to also be concerned with application level security. A very common issue in cloud security currently is insecure application programmer interfaces (APIs). These APIs allow on-demand self-service by providing ease-of-use for a customer to scale resources as necessary without having to contact human support. However, CSP APIs, according to Srinivasan et al., "can also invite attackers attention to know the architecture of the CSP and internal design details, if not completely but to a greater extent. Hence, insecure APIs may lead to major security concerns for the CSP...such as illegitimate control over user accounts, etc." [3]

Finally, implementing all the appropriate technological defenses will never prevent simple social engineering attacks. One attack the Cloud Security Alliance discusses is the threat of a malicious insider. It states that "this threat is amplified for consumers of cloud services by the convergence of IT services and customers under a single management domain, combined with a general lack of transparency into provider process and procedure." [5] The Cloud Security Alliance also notes that there is often very little visibility into the hiring process of cloud employees and that an adversary anywhere from a hobbyist hacker to a nation-state sponsored intruder could be accidentally hired.

Conclusion

It is clear that the attractive benefits of cloud computing does not come without its security complications. Customers sharing the same resources owned and managed by a separate party leads to less control over security, a larger attack surface, and an increased velocity of attack. This paper is certainly not a comprehensive study of every single security measure that should be taken in a cloud environment, but it does layout some good practices that should be followed, and more importantly, it outlines the additional complexity and extra points of security failure that are present in the cloud. Customers should first carefully consider the amount of control over the data they need before an appropriate service and deployment models necessary. Also, they should

carefully choose a reputable CSP that emphasizes security because a breach in the cloud can lead to brand damage, financial impact, and productivity losses. Therefore, as more and more data gets pushed to the cloud, more attention should be shifted toward taking all steps necessary to secure this precious data.

References

[1] Bisong, A., & Rahman, S. (2011). An Overview of the Security Concerns in Enterprise Cloud Computing. *International Journal of Network Security and Its Applications, 3*(1). doi:0.5121/ijnsa.2011.3103

[2] EMC Corporation. (2014). Module 14: Securing the Storage Infrastructure. In Information and Storage Management V2: Summer 2015. Retrieved from https://education.emc.com/

[3] Srinivasan, M., Sarukesi, K., Rodrigues, P., Manoj M, S., & P, R. (2012). State-of-the-art Cloud Computing Security Taxonomies ± A classification of security challenges in the present cloud computing environment. *Proceedings of the International Conference on Advances in Computing, Communications and Informatics*. doi:10.1145/2345396.2345474

[4] The NIST Definition of Cloud Computing. (2011, September 1). Retrieved December 15, 2015, from http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf

[5] Top Threats to Cloud Computing V1.0. (2010, March 1). Retrieved December 15, 2015, from https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[6] Winkler, V. (2011, December 1). Cloud Computing: Virtual Cloud Security Concerns. Retrieved December 15, 2015, from https://technet.microsoft.com/en-us/magazine/hh641415.aspx