Private Virtual Infrastructure for Cloud Computing

F. John Krautheim
University of Maryland, Baltimore County, 1000 Hilltop Circle, Baltimore, MD 21250
john.krautheim@umbc.edu

Abstract

Cloud computing places an organization's sensitive data in the control of a third party, introducing a significant level of risk on the privacy and security of the data. We propose a new management and security model for cloud computing called the Private Virtual Infrastructure (PVI) that shares the responsibility of security in cloud computing between the service provider and client, decreasing the risk exposure to both. The PVI datacenter is under control of the information owner while the cloud fabric is under control of the service provider. A cloud Locator Bot pre-measures the cloud for security properties, securely provisions the datacenter in the cloud, and provides situational awareness through continuous monitoring of the cloud security. PVI and Locator Bot provide the tools that organizations require to maintain control of their information in the cloud and realize the benefits of cloud computing.

1 Introduction

Cloud computing is poised to revolutionize computing as a service. With the ability to provide on-demand computing resources dynamically, companies can fundamentally change their information technology strategy. As with any new technology, this new way of doing business brings with it new challenges, especially when considering the security and privacy of the information stored and processed within the cloud.

Cloud computing utilizes massively scalable computing resources delivered as a service using Internet technologies. Cloud computing allows these computational resources to be shared among a vast number of consumers to allow for a lower cost of ownership of information technology.

The Infrastructure as a Service (IaaS) model of cloud computing [1] provides on-demand online computing infrastructure resource at a reduced overall cost of ownership. The IaaS model makes all of the facilities required for a datacenter application available over the Internet which clients purchase as an outsourced service. Companies are turning to the cloud for datacenter services to improve scalability and global reach, and to lower overhead. But as they do, they must proceed cautiously and evaluate all risks and issues carefully.

One of the risks of cloud computing is that the users, who are the information owners, lose control of their data when they release the information into the cloud for processing. Relinquishing physical control of the datacenter infrastructure and information increases the risk of data compromise considerably [2]; however, the benefits of moving to cloud computing for services may be significant enough to justify the risk. These benefits include lower operating costs, physical space savings, energy savings and increased availability [3].

Ensuring the security and integrity of information in the cloud becomes an issue as the management and ownership of the hosting platforms is removed from the consolidated control of a single facility and a single owner. Many organizations such as financial institutions, health care providers, and government agencies are legally required to protect their data from compromise due to the sensitivity of their information. Generally, these organizations are required to manage and maintain their own datacenters with stringent physical and logical protection mechanisms ensuring that their data remains protected. These organizations simply cannot utilize cloud computing in a generic manner due to the inherent risk of data compromise from systems they do not control.

To date, there has been minimal research published on cloud computing security. This paper introduces new research in a cloud management and security model called *Private Virtual Infrastructure* (PVI). PVI allows organizations to utilize cloud resources with the level of assurance that is required to meet their confidentiality concerns. PVI is based on five tenets we propose as a basis for cloud security. By sharing the responsibility for security between the service provider and the customer, PVI reduces the risk of using cloud computing services. By using PVI and applying the five tenets of cloud security, organizations can

maintain control of their information in the cloud and realize the benefits cloud computing provides.

2 Security in the Cloud

Cloud security requires total situational awareness of the threats to the network, infrastructure and information. One of the biggest advantages to the cloud's utility, abstraction [4], is also its biggest security weakness. Abstraction allows the cloud to be pervasive and removes knowledge of the underlying fabric of processors, storage, and networking; however, without knowledge of the underlying fabric, information owners' understanding how to secure their applications and information becomes very complex. Many of the security principles used today to secure datacenters and networks rely on the information owners' ability to manage the underlying fabric of servers, routers, firewalls, and intrusion detection devices to understand when attacks are occurring and to responds to the threats by shutting down access to resources and isolating pieces of the fabric that are being attacked.

In a cloud, traditional security methodologies do not work as the service providers cannot allow information owners, or clients, to manipulate the security settings of the fabric. If this were allowed, it would be possible for one client to change security settings illicitly in their favor, or change security settings of other clients maliciously. This situation is unacceptable since the information owner cannot manage the security posture of their computing environment. Therefore, a security model is needed that allows for an information owner to protect their data while not interfering with the privacy of other information owners within the cloud.

The cloud requires a new model for handling security, one that is shared between operators and clients. Operators need to give clients visibility into the security posture of the fabric while maintaining control. The clients need to have assurance that they can control the privacy and confidentiality of their information at all times and have assurances that if needed, they can remove, destroy, or lock down their data at any time.

A method of combining the requirements of the user and provider is to let the clients control the security posture of their applications and virtual machines while letting the service provider control the security of the fabric. This provides a symbiotic security stance that can be very powerful provided both parties hold up their end of the agreement.

3 PVI Cloud Security Model

Private Virtual Infrastructure meets the goals of a shared security posture where all resources necessary for the virtual datacenter are securely isolated from the greater cloud. PVI provides secure provisioning of commodity internet resources isolating the client's datacenter to operate in its own virtual domain.

The PVI cloud security model is a virtual datacenter over the existing cloud infrastructure. This virtual datacenter is under control of the information owner while the fabric is under control of the operator. Both parties must agree to share security information between themselves and possibly other parties in the cloud to achieve situational awareness of the security posture at all times.

The service level agreement between the client and provider is critical to defining the roles and responsibilities of all parties involved in using and providing cloud services. The service level agreement should explicitly call out what security services the provider guarantees and what the client is responsible for providing. Clients should thoroughly examine and negotiate the Service Level Agreements with their vendors to determine and minimize their risk exposure before agreeing to use any cloud computing service.

Adding security to any system inevitably leads to a compromise in some fashion. For PVI, the abstraction of the fabric is removed. It is impossible to have a completely obscure fabric for IaaS that provides the assurances of security properties required for the sensitive data contained in a PVI.

In order to verify the security within the cloud, each service in the cloud needs to be able to report security properties present and the report must be verifiable. These properties must be cryptographically bound and signed such that anyone wishing to verify the properties, and has the proper authorizations, can do so. This ability means that clients need visibility into the security settings and configuration of the fabric. We have chosen to use trusted computing techniques to verify these settings and report the configuration of the fabric in PVI.

Additional requirements for PVI are that communications to and within PVI should be done through virtual private networking and all links should be encrypted with IPsec or SSL tunnels. This step provides confidentiality on the network and prevents other users within the cloud from eavesdropping and modifying communications of PVI.

3.1 Trusted Computing

Trusted computing provides mechanisms to control the behavior of computer systems through enforcement of security policies via hardware and software controls. By requiring service providers to use trusted computing technology, organizations can verify their security posture in the cloud and control their information, allowing them to achieve the economies of scale, availability, and agility that the cloud promises.

A key component of trusted computing is the Trusted Platform Module (TPM). The TPM is a cryptographic component that provides a root of trust for building a trusted computing base. The TPM stores cryptographic keys that can be used to attest the operating state of the platform. The keys are used to measure the platform, which are then stored in the TPM's Platform Configuration Registers (PCRs). The attestation process allows clients to request the PCRs of the TPM and verify that the platform they are using meets their policy and configuration requirements. The client can then determine whether they wish to utilize the service provided based on the attestation from the platform's TPM.

One problem associated with the TPM is that it only works for non-virtualized environments. If virtualization is used, which is a common occurrence in cloud services, the TPM also needs to be virtualized. For this reason, specifications have been developed for a virtual TPM (VTPM) [5]. The VTPM is implemented by providing software instances of TPMs for each virtual machine (VM) on a trusted platform [6].

PVI uses TPMs as the basis for trust in the cloud. Individual computing platforms within the cloud each have a TPM owned by the service provider. VTPMs are linked to the physical TPM and used to secure each VM in the cloud. We developed an architecture that cryptographically secures each VM by tightly coupling a VTPM in its own stub domain called a *Locator Bot* (LoBot) [7]. LoBot allows each VM to be verifiable by its owner and provides secure provisioning and migration of the VM within the cloud as well.

3.2 Tenets of Cloud Security

In order to provide a secure framework for IaaS, we propose the following five basic tenets to cloud security:

1. Provide a trusted foundation on which to build PVI. This is accomplished through the service level agreement with the service provider assuring they will provide the requisite security services necessary to protect the information with PVI.
2. Provide a secure factory to provision PVI. The factory also serves as a policy decision point and root authority for PVI.
3. Provide a measurement mechanism to validate the security of the fabric prior to provisioning of PVI.
4. Provide secure methods for shutdown and destruction of virtual devices in PVI to prevent object reuse attacks.
5. Provide continuous monitoring and auditing from within PVI as well as from outside of PVI with intrusion detection systems and other devices.

These tenets of cloud security will allow us to increase the security posture of cloud computing. Through universal adoption of these tenets, many of the security concerns associated with cloud computing become much easier to handle. Section 4 provides an in-depth look at how we can leverage these tenets to increase the security posture of the cloud.

4 PVI Cloud Security Architecture

The Private Virtual Infrastructure architecture has two layers that separate the security responsibility between the service provider and the client. The IaaS fabric layer provides computation resources managed by the service provider, while the PVI layer provides a virtual datacenter managed by the client. The service provider assumes responsibility for providing the physical security and the logical security of the service platform required for the PVI layer.

Each client is responsible for securely provisioning their virtual infrastructure with appropriate firewalls, intrusion detection systems, monitoring and logging to ensure that data is kept confidential. PVI enables the client to build a virtual infrastructure that meets these requirements. We now discuss how the basic tenets of cloud security are implemented to enable PVI to provide the data protection required.

4.1 Trusted Cloud Platform

One of the key foundations for the PVI security model is the ability to verify security settings of the underlying fabric. The provider needs to provide security services which protect and monitor the fabric. These services can be reported via an identity certificate presented to the virtual environment that attests these services. This reporting could be accomplished in many different manners. PVI relies on trusted computing components to achieve the trusted cloud platform.

There are several research projects and products built on trusted computing platforms which we can leverage to build a trusted foundation for PVI. IBM's Trusted Virtual Datacenter (TVDc) [8] provides many features that can be used in a cloud computing environment for securing a datacenter management and VM isolation through their secure hypervisor called sHype. TVDc builds upon Trusted Virtual Domains [8], which provides strong isolation and integrity guarantees that significantly enhance the security and management capabilities in virtualized environments. These solutions provide a solid foundation for building a virtual datacenter in the cloud.

4.2 PVI Factory

The PVI Factory is the most sensitive component of the PVI. The factory is where all components of the

PVI are provisioned and it is the root authority for provisioning, VTPM key generation, and certificate generation and management within the PVI. The factory also maintains master images for application servers, and handles data transfers to the PVI through the VPN configuration and management.

Since the factory is the root authority, if it is compromised, then all existing PVI components are at risk of compromise and future provisioned components cannot be trusted. Therefore, the PVI factory should be under full control of the information owner, either as a standalone component in the datacenter or on the information owner's site. It should not be virtualized and should be isolated to the greatest extent possible from other systems. Ideally, it would have built-in hardware to accelerate cryptographic operations and to provide true randomization, but a software-only implementation would suffice for most applications.

The PVI factory serves as the controller and policy decision point for the PVI. It is responsible for ensuring the integrity of the PVI and handling incidents in the event of a security breach. If any problems are detected, it should shutdown the PVI, recall and inspect all images for tampering, and generate alarms and reports.

4.3 Measurement and Secure Provisioning

Removing the abstraction of the fabric is a trade off that we must be willing to take to increase the security of the virtual datacenter. This means that service providers must allow clients transparent insight into their infrastructures. Most providers today do not want to provide details about their inner workings as they fear this will remove their competitive advantage; however, we feel that providing a synergistic relationship with their customer base can also be their competitive advantage.

Fabric pre-measurement is what allows PVI to share the responsibility of security management between the service provider and client. Pre-measurement is performed by a LoBot, which tests the fabric's security posture before provisioning occurs, allowing the information owner to determine the safeness of the fabric before deployment of a PVI.

LoBot is a VM architecture and secure transfer protocol based on VTPMs. After LoBots probe target platforms for security properties they can securely provision VMs on those platforms. A LoBot is a self-contained virtual machine with a VTPM and probe application that is provisioned on a target machine. Upon startup, the VTPM binds itself to the target's TPM, and then the probe application reads the platform configuration from the target TPM's PCR and obtains identifying information about the platform. Identity information is provided in the form of certificates. This information is then combined with the VTPM's PCR which is cryptographically sealed in a blob that is transferred to the PVI factory.

The PVI factory decrypts the blob and examines the information received to determine whether the environment is safe. Once the target environment is determined to be safe, the PVI factory configures the VM and securely transfers it to the target environment, via the LoBot protocol, in a blob encrypted such that only the target platform may execute source environment.

At the target environment, the LoBot probe application receives and unseals the source environment. If the source environment was tampered with during transfer, it will be detected during the decryption phase. To make sure everything is safe, the probe measures the source environment one more time to validate its integrity and to ensure the launch in the target environment was successful.

4.4 Secure Shutdown and Data Destruction

Since PVI runs on shared hardware platforms, secure shutdown and data destruction is required to ensure all sensitive data is removed before new processes are allowed to run on it. All memory used by virtual machines should be zeroized such that object reuse attacks [9] are thwarted.

Today's virtual machine monitors do not provide secure shutdown or data destruction capabilities. A vulnerability arises when a VM with sensitive information is shut down and a new VM is provisioned with the same memory space. The new VM could simply read its entire memory space looking for data left behind by the previous VM. The security and privacy implications of such a threat are very serious as many organizations process sensitive information that can be stolen and used for identity theft, fraud, blackmail, and other illicit activities. We recommend that secure shutdown and data destruction capabilities be built into future virtual machine monitors; however, we believe that through LoBot, we can provide the capability to wipe a virtual machine's memory space securely after shutdown thus eliminating any data that may have been left behind by the virtual machine.

4.5 Monitoring and Auditing

Another capability LoBots provide is continuous monitoring of the cloud environment. Since each VM within PVI has an associated LoBot, the LoBots can continually monitor the cloud environment and communicate among themselves and the PVI factory to achieve situation awareness of the cloud environment. The LoBot network can perform this duty with minimal interference to PVI operation greatly increasing the security posture of the virtual datacenter.

Auditing within PVI increases the ability to handle security incidents. With the vast number of users and

the amount of information within the cloud, forensic capability is diminished by the sheer volume of information to process [2]. We recommend the sharing of auditing responsibilities between the service providers and clients to provide an increased ability for forensic analysis.

Monitoring and logging should be done within PVI in addition to the security monitoring and services provided by the fabric. This increases the forensic capability to investigate security incidents at both levels of the system. Reconciliation of the PVI and fabric logs can enhance the ability and speed of tracking down incidents.

5 Ongoing Cloud Security Research

There are several projects we are working on for securing cloud computing fabrics. First LoBot [7] is our architecture and protocol for secure provisioning and secure migration of virtual machines within an IaaS cloud. LoBot provides many other security features for PVI such as environmental monitoring, tamper detection and secure shutdown.

We are also researching identification of virtual machines throughout their lifecycle called Trusted Virtual Machine Identification, which uses cryptographic identity certificates bound through VTPMs to manage virtual machines in the datacenter. Identity certificates can also be used to identify the host platform and services provided as well. The identity certificate provides a unique identity to each virtual machine that is maintained throughout the lifetime of VM. The information maintained about the VM includes its creation date, migration and cloning data, and other operating statistics vital to managing the virtual datacenter.

With the combination of Private Virtual Infrastructure, LoBot, and Trusted Virtual Machine Identification we have a powerful toolset to tackle security and management issues in the cloud computing environment. When combined with other research projects such as TVDc and VTPMs, building secure cloud environments is easily realizable.

6 Conclusion

This paper proposes a new paradigm for securing and managing cloud computing services based on a synergistic relationship between the vendor and customer of cloud services. This relationship provides an increased security posture while allowing both parties to set security controls required to protect the infrastructure and data within the cloud and virtual datacenter.

Cloud computing service providers need to enable a transparent view of their infrastructure so their customers can understand the security posture and threats to the system. We feel that this capability will give the vendor a competitive advantage as a secure system provider over vendors who choose to obscure their infrastructure inner workings to protect proprietary technology. In the end, cooperation between vendor and customer will result in increased security while lowering the overall cost of ownership for IT infrastructure.

Security is the responsibility of all parties involved in IaaS cloud computing. Vendors are responsible to provide a secure fabric. Information owners are responsible to protect their data. By following the five tenets of cloud security, PVI provides information owners the flexibility to manage their own data while realizing the cost benefits of cloud computing.

Acknowledgement

This work is performed under a grant from the Department of Defense Information Assurance Scholarship Program. Special thanks goes to my advisors Dhananjay Phatak and Alan T. Sherman for their support. Reviews and comments from Russell Fink and Richard Carback were especially helpful.

References

[1] J. Leach, "The Rise of Service Oriented IT and the Birth of Infrastructure as a Service," March 20, 2008; http://advice.cio.com/jim_leach/the_rise_of_service_oriented_it_and_the_birth_of_infrastructure_as_a_service.

[2] J. Heiser and M. Nicolett, *Accessing the Security Risks of Cloud Computing*, Gartner, Inc., Stamford, CT, 2008.

[3] M. Armbrust, A. Fox, R. Griffith *et al.*, *Above the Clouds: A Berkeley View of Cloud Computing*, Unversity of California, Berkeley, Berkeley, CA, 2009.

[4] D. Nurmi, R. Wolski, C. Grzegorczyk *et al.*, *Eucalyptus: A Technical Report on an Elastic Utility Computing Architecture Linking Your Programs to Useful Systems*, Technical Report 2008-10, University of California, Santa Barbara Computer Science, Santa Barbara, CA, 2008.

[5] S. Berger, R. Cáceres, K. A. Goldman *et al.*, "vTPM: Virtualizing the Trusted Platform Module," in Proceedings of the 15th USENIX Security Symposium, Vancouver, B.C., 2006.

[6] V. Scarlata, C. Rozas, M. Wiseman *et al.*, "TPM Virtualization: Building a General Framework," *Trusted Computing*, N. Pohlmann and H. Reimer, eds., pp. 43-56, Wiesbaden, Germany: Vieweg+Teubner, 2008.

[7] F. J. Krautheim and D. S. Phatak, "LoBot: Locator Bot for Securing Cloud Compupting Environments," submitted 2009 ACM Cloud Computing Security Workshop, Chicago, IL, 2009.

[8] S. Berger, R. Cáceres, D. Pendarakis *et al.*, "TVDc: Managing Security in the Trusted Virtual Datacenter," *ACM SIGOPS Operating Systems Review*, vol. 42, no. 1, pp. 40-47, January, 2008.

[9] H. Tipton and K. Henry, *Official (ISC)^2 Guide to the CISSP CBK*, Boca Raton, FL: Auberbach, 2007.