Evaluating Security Mechanisms Implemented on Windows Azure

Alexander Akinbi, Ella Pereira, Chris Beaumont
Edge Hill University, United Kingdom

Abstract

Slow adoption of cloud services due to security concerns indicates a need for evaluating existing security measures in cloud and further development of methods and techniques for their enhancement. This paper presents an investigation into the security mechanisms of Windows Azure, Platform-as-a- Service (PaaS) delivery model. The evaluation in this case study is achieved by segregating the cloud service into three core components and then assessing each using a taxonomy for PaaS cloud security made up of operation domains identified by the Cloud Security Alliance (CSA) and our developed security framework as matrices. This work aims to look at the holistic security architecture of PaaS cloud service in order to identify its security offerings and develop a security risk profile. The preliminary results indicate that most vulnerable component of PaaS, Windows Azure, and possibly in other clouds too is the Host/Compute component, responsible for the application and visualization security.

1. Introduction

A study conducted by the Ponemon Institute, 2010, on the Security of Cloud Computing Users Study, concluded that 46 percent of IT professionals in the study indicated that their organizations are skeptical on the adoption of cloud computing due to security concerns [15]. Their findings concluded that cloud service providers are not focused on cloud security. Rather, their priority is to deliver the features their customers want such as low cost solutions with fast deployment that improves customer service and increase the efficiency of the IT function [15]. Their later study in 2012 revealed that an average of 4,140 business and IT managers surveyed in Europe, America and Asia responded they are unsure what their cloud providers are doing to protect their organization's data in the cloud [16].

In cloud computing, the security controls implemented and integrated are not different to traditional information systems however cloud computing presents different risk compared to tradition information systems due to virtualization and management control of the architecture. In PaaS public cloud environments, security is a shared responsibility, where the platform's security is provided by the provider but the developed web based application's security is the responsibility of the customer [1].Cloud providers offer the underlying infrastructure, compute and storage resources needed for the development of web based applications as well as management and control over these resources they provide which include security. However unless these providers disclose the security controls implemented to what extent they are integrated to their customers, the customer will not know which controls are needed to maintain the security of their assets. There is tremendous potential for misguided risk management decisions which could be detrimental [1].

Security publications such as the NIST [4] CSA [1] provide us with recommendation for selecting security controls and guidelines for critical areas on information systems which includes cloud computing. However knowing how these security controls integrate to meet stated security requirements can only be achieved by evaluating the controls implemented on them. A study in [17] suggests that security standards such as ISO 27001:2005 are not completely adequate to address challenges posed especially by virtualization which cloud computing offers.

Hence the purpose of this paper is to evaluate the security controls implemented on a PaaS public cloud, Windows Azure, by evaluating its security mechanisms and offerings against a security framework developed using industry security standards, guidelines and publications to determine which controls exist and which do not exist on each component of the cloud architecture. With the risk and vulnerabilities associated to each PaaS cloud component, the author intends to determine what security controls are implemented to reduce the identified risks in achieving adequate security requirements on this type of cloud service delivery model. The use a security framework as described in [2] helps in mapping out how the security on PaaS on each component of the cloud are integrated in relation to industry compliance models for choosing and implementing effective security controls.

The remainder of this paper is as follows: In Section 2, we present taxonomy for Platform-as-a-

Service cloud security by discussing this cloud service delivery model domains and how they relate to its components. Section 3 highlights the architecture components of Windows Azure. Section 4 discusses the strategy and evaluation of security mechanisms implemented on Windows Azure. The security risk profile of Windows Azure is discussed in section 5 while a conclusion of the work done is presented in Section 6.

2. Taxonomy for PaaS Cloud Security

Beyond the architecture of PaaS cloud environments, the CSA focuses security guidance on two broad domain categories of cloud computing environments. The governance domain discusses the policy issues around cloud computing environment while the operational domain discusses the tactical security concerns and implementation within the architecture. Using this guidance, our security strategy is focused around the operational domain, which highlights guidance with application security, identity and access management, encryption and key management as well as virtualization security of a PaaS public cloud environment, all of which are based on technical security considerations.

Each aspect under the operational domain category is linked to specific components of PaaS in providing computation resources and storage environment for the development of web based applications.

Application Security: This involves the security of applications developed, running and deployed within the PaaS host component. Application security on the cloud is the sole responsibility of the developer to ensure the application is not vulnerable to attacks due to unsecured communication or access during utilization of the application by end users. These kinds of attacks must be defended by the application itself. Typically, using secure program logic and secure coding [5] best practices in the software development lifecycle of the application. On the other hand, the security of stored data applications and source code before they are deployed to end users should be provided by cloud providers to mitigate the risks of data modification or unauthorized access to stored objects.

Data Storage Security: This relates to security of logical storage container such as object/file storage, databases or VHDs, where data/ application are stored or archived on a digital storage location The entire data security lifecycle as described in [9] incorporates two aspects of where the data is located and who has access to these storage location from the creation of data to its sharing or destruction. In our framework [2], we highlighted the monitoring and encryption of data in transit at the host component of PaaS and also on the storage component of data at rest. Security controls and implementation that mitigate risks of data leakage, modification, vulnerable host operating system, virtual machine and hypervisors must be provided by cloud providers on these components of the cloud. Data stored however must not be stored in clear text [3] but encrypted using industry standard cryptography techniques and encryption/decryption keys properly managed [12] [13].

Authorized access to data stored on PaaS requires a secured channel via the API which is more or less highlighted in the identity and access management implemented on this channel.

Identity and Access Management: This refers to the management of individual identities, authentication, authorization and access to assets in an information system governed by policies and controls with appropriate privileges within the system. In PaaS, customers have access to the environment via a web portal or management API. In this cloud delivery model, the provider is responsible for managing access control to the network, servers and application platform infrastructure. However, the customer is responsible for access to application placed on the PaaS platform [7]. The whole identity and access management encompasses the ability of the PaaS and controls implemented to confirm and manage the life cycle of an assured identity (human/device/process), assigned properties of entities, manage permissions to perform an action in the cloud and also manage the lifecycle of digital credentials through authentication [9]. In multi-tenant cloud environments such as PaaS, providers must segregate customer identity and authentication information while the identity and access management components should also be easily integrated with other security components on the cloud [11].

Encryption and Key Management: Encryption of data before storage in the cloud is essential on public clouds due to the multi-tenant model. Ability to utilize cloud storage controls perhaps built in controls to enable encryption and segregation of data. One of the most difficult processes in public cloud computing typical to PaaS, is the management of symmetric or asymmetric keys used in the encryption of data. Maintaining proper key management and storage from unauthorized users is essential for security of data stored on public clouds. Although data encryption helps protecting data confidentiality, it also obsoletes the traditional data utilization service based on plain text keyword search. Thus, enabling an encrypted cloud data search service with privacy-assurance is of paramount importance [10]. On the other hand, keeping encrypted copies of same data in the cloud may affect system performance and incur high computational cost

[14].

Virtualization Security: Virtualization is the concept by which cloud computing is established. It is the mechanism that abstracts the coupling between the hardware and operating system [8] by presenting the host platform virtually. Basically virtualization in the cloud is of different types which include server, storage and network virtualization [8]. Having virtual machines run on the cloud brings about various challenges as well. Encryption of virtual machine images to prevent modification and theft at rest or when they are running. Access through virtualization to resources and service running in the cloud requires protection against failovers through hardware load balancing. However, CSA [1] suggests providers have tried to satisfy virtualization security as a service on a cloud platform but because these services take many forms and lack transparency regarding deployed security controls, they have caused market confusion and complicated the selection process of adequate controls.

Figure 1 shows the operational domains which revolve around PaaS cloud service delivery model. Security mechanisms and controls implemented of this type cloud service must be able to meet specific security and management requirements for each of the domains.

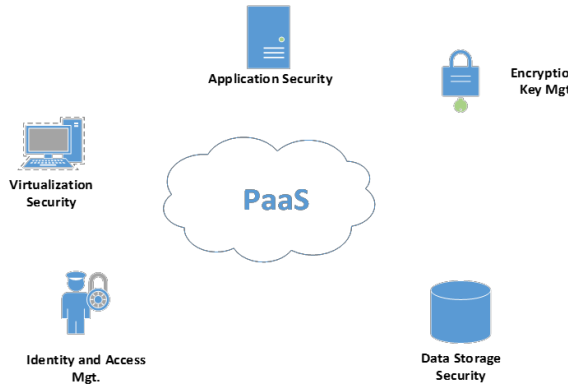

Figure 1. Taxonomy for PaaS Security Controls

3. Segregating Windows Azure Architecture Components

To understand security offerings provided on Windows Azure, it is essential to divide the PaaS into its architecture components. Windows Azure [22] offers an insight into its components by grouping its components into distinctive categories based on services it offers rather than security architecture. However a security overview it shares in a publication [21], gives us a clear understanding on how its architecture can be divided into its PaaS components. Using our segregation template for generic PaaS components shown in Table 1, we divided Windows Azure into three components, Table 2, in order to assess the security controls implemented on each component of its cloud architecture.

Table 1. Generic PaaS Components

Component I: **Developer environment**	**User Interface**
	Middleware
Component II: **Host**	**VMs and Guest OS**
	Hypervisor
Component III: **Back End**	**Logical Storage**
	Network

Developer Environment: The upper layer of our PaaS component segregation is made up of the user interface and middleware which is described as the interface that enables the customer or developer to interact with the PaaS host layer in order to manage, develop and deploy services or applications. In Windows Azure, the component is made up of a subscription account and an application programming interface (API) for customers to manage applications and storage [21]. As described in [21], access to the web portal is via the subscription which is created during the registration for the PaaS account. The user is only able to access the PaaS using the API provided by the CSP or using an open standard API, such as a web browser, which is compatible with the PaaS as recommended by the service provider [2].

In Windows Azure, the API is referred to as a Service Management API (SMAPI). Access to the PaaS storages or services is through the SMAPI over web services which enable customers to manage their storage accounts and deployed applications. Access can also be made through programming API command lines downloaded and installed via the software development kit (SDK) such as Virtual Studio Web Express. A service that provides just user management access through a web browser alone is regarded as a Software- as-a-Service (SaaS) but alternatively through a command line API is a PaaS. The subscription account contains of a unique identifier that enables calls to be made to the SMAPI for service operations within the cloud environment.

The Windows Azure App Fabric on the other hand, constitutes the runtime and middleware component of the developer environment. This middleware consists of pre-built services and runtime engine that allow developers to build applications easily, leverage various communication protocols between applications on the cloud and enables an easy way to provide identity and access control to web applications and services, while integrating with standards-based identity providers [6].

Host/Compute Component: This component consists of the hypervisor and compute nodes for creating instances which are run on virtual machines. The guest operating system run on individual VMs created, which are all managed by the fabric controller located below the host/compute component. The hypervisor also knows as Hyper-V in Windows Azure, in turn isolates the VM instances running to create sandboxes or isolated multi-tenants. The purpose of a hypervisor is to present to the guest VM a view that appears as though the operating system and applications inside the VM are running directly on some given hardware [19]. This is also known as abstraction. Therefore the hypervisor serves the role of a virtual machine manager (VMM) in presenting each VM with a guest OS which they can run. Programming source codes are run and executed on this component before deployment.

Back End Component: As discussed in Section 2, data storage on PaaS are stored on object/files storage, databases or virtual hard drives. In Windows Azure, this component is made up of tables, queues, blobs and storage emulator which serve the same purposes. Tables, queues and blobs are logical virtual storages in the cloud that can be accessed and managed through the SMAPI while the storage emulator is Windows Azure storage, a replica of tables, queues and blobs, simulated on the customer's local machine. While the cloud storage services which include tables, queues and blobs serve as backend storages for applications deployed and running in the cloud, the storage emulator is not scalable and best suited for testing the functionality of developed applications on the customer's development machine before they are deployed onto the cloud service.

Table 2. Windows Azure Components

Component I: Developer environment	Subscription Web Portal/ SMAPI
	App Fabric
Component II: Host/ Compute	VMs and Guest OS
	Hyper-V
Component III: Back End	Tables, Queues, Blobs, Emulator
	Fabric Controller

The storage component also consists of the fabric controller (FC). The FC is responsible for allocating disks space and network to role instances of VMs created on the host/compute component. It is the nucleus of the entire Windows Azure PaaS. It manages deployment of guest operating system images and resources as they are provisioned to run on VMs by the customer. The FC performs virtual tailored networking operations that link the tables, queues and blob storages with the hypervisor and the cloud core infrastructure components.

4. Evaluation of Windows Azure Security

The strategy used in this study is based on the use of the taxonomy for PaaS security discussed in Section 2 to evaluate each component of Windows Azure. This strategy enabled us assess security mechanisms that exist and where they are implemented on the cloud platform and how each security mechanism is integrated to ensure confidentiality, integrity and availability of assets and resources in the cloud. We measured each component by the security requirement based on the implemented taxonomy for PaaS cloud security, security aspect and security method according to our existing security framework as described in [2]. This process was carried out by monitoring our existing Windows Azure account subscription for the security offerings provided to meet security requirements expected in the taxonomy.

Developer Environment Security: Windows Azure offers Windows Live ID and a self-signed certificate as authentication mechanisms to provide identity and access management to the cloud service. The cloud service subscription is registered with a Windows Live ID associated to the customer's credit card detail. It is setup with an email address and password used to create a Windows account and is authenticated by a Microsoft authentication server once the credentials are sent via a SSL connection. In Windows Azure, the SMAPI and web portal are built upon the Representational State Transfer (REST) protocol. This involves the use of HTTP requests such as GET, POST, PUSH and DELETE to make calls or execute commands and operations. A secure SSL communication is established using asymmetric cryptography or public key encryption which provides encryption of credentials sent between the customer's web browser and the Microsoft authentication server.

Moreover, Windows Azure provides multifactor authentication or two factor authentication using various techniques to manage identity and access to the customer web portal. For instance, it provides an option to allow a customer sign in using a single-use code or one time password (OTP). This requires sending the code to the user's phone via SMS to prevent password theft when a customer uses a public computer. This authentication mechanism is not available by default unless the user chooses to sign in using this method at the sign in webpage. An administrator can also configure multifactor authentication to verify other end users' sign-ins using a mobile app, phone call or text message to the cloud service. Windows Azure also allows administrators to configure their own premise active directory to authenticate users using existing controls and policy access to the cloud service. This configuration can be managed through the Windows

Azure web portal to implement these settings.

The App Fabric on the other hand is made up of software libraries that provide identity and access control services capabilities to web applications using active directory and other web service identity provides such as Google, Yahoo and Facebook [17]. In other words, this service component enables customers implement application security using federation and trust industry standards. This added functionality enables developers to implement security controls on how their end users interact with web based applications hosted on the cloud service and how their web based applications authenticate end users. It supports the use of X.509 certificates, REST protocol, ADFS and standards such as OAuth, W3C, WIF-Security, and WS- Trust for implementing Security Token Service (STS). This service component provides role based access control (RBAC) and claim based authorization capabilities. The service can be implemented via the web management portal of Windows Azure.

Host/Compute Security: Virtualization security is provided on this component by providing VM security, OS hardening and Hypervisor security. Although users are not given full administrative privileges to their VMs, security can be enhanced as an administrator can create a boundary of IP addresses to restrict unauthorized access to VMs deployed and running in the PaaS cloud. This is referred to as establishing endpoints or creating subnets. VM isolation or segregation is provided by the hypervisor (Hyper-V) coupled with the network functionality of the FC. Isolating VMs on Windows Azure is enhanced by allocating individual fixed private IP addresses to VMs created within a cloud service subscription. This ensures only VMs within that cloud service can communicate with each other, hence a technique in resolving multi-tenancy while access to the internet is provided, using a single public IP address. Closing and opening only specific ports also can be used to secure VM communication.

Operating system hardening requires making sure the operating system is not exposed to vulnerable attacks. Windows Azure through its software development lifecycle and implementation provides three local VHDs labeled C: D: and E: in the root OS file system for each VM created. The D: and E: virtual drives are read-only by default and do not allow write processes. The D: VHD contains one of several versions of the Guest OS kept up to date with the most current patches while the E: virtual drive contains an image constructed by the FC based on the package provided by customer [18]. This ensures that regular updates can be made to the VHDs to harden the OS and improving the OS security as a whole. The C: virtual drive is the only read and write disk where the configuration file is stored as provisioned by the FC when the customer makes changes during configuration of the Guest OS.

A vulnerable VM exposes threats to the hypervisor due to the constant communication between the Hyper-V (VMM) and guest VMs. Therefore, to secure the hypervisor, Windows Azure uses VLANs to prevent packet sniffing by a compromised VM on other guest VMs within the cloud service. This also helps protect the hypervisor from spoofing attacks or DDOS attack. Firewalls are integrated to provide intrusion detection and intrusion prevention once a VM has been compromised and all communication between the logical storage, hypervisor and guest VMs are done over SSL secure communication.

Back End Security: Windows Azure provides data security for the storage emulator and cloud storage services by ensuring that the .NET cryptography techniques such as PKI encryption, decryption and hashing can be implemented to secure data stored and transmitted on the local machine using Virtual Studio Web Express. Therefore customer themselves must provide data storage security using cryptographic techniques they are used to in tradition information systems. Cryptography and hashing mechanisms such as symmetric key encryption (AES), asymmetric PKI infrastructure, SHA-1, SHA-2, and MD5 hashing are all recognizable.

According to Windows Azure [22], the storage emulator supports the use of a single account name and key which are simply credentials to use with the storage but do not provide identity and access management. By default, Windows Azure provides the account name and key which cannot be used to access the cloud storage services. Access to these cloud storages is recommend via HTTPS and requires a pair of storage account keys, primary and secondary keys. Each key is a 512 bit storage key used for authentication when the storage account is accessed. The primary key is used for authentication while the secondary is used in place of the primary key until new sets of keys are generated. Customers can generate new sets of keys each time to avoid the keys being compromised by an attacked but will have to deploy the new key to applications that use cloud storage services as backend where initially the old keys have been configured to use to access the cloud storage services. For instance, when a developer renews the primary key, application using the key could use the secondary key pending the time a new key is generated to save downtime.

However, since encryption is not an issue for developers, key management becomes an issue as applications will need keys to access data and will require the keys to always be stored within the cloud storage services. Preserving the confidentiality of customer's credentials to the web portal and storage access keys becomes the sole responsibility of the user as leakage will make the cloud service vulnerable.

Also keys used to encrypt/decrypt data are exposed once an attacker gains access to storage access keys. Therefore storage component security depends on the security enforced by the developer on web based applications running in Windows Azure. The FC maintains the availability of OSes, and hypervisor provisioning VMs. It enables seamless changeover should the datacenter hosting a customer's cloud service fails by networking datacenters. Windows Azure provides security to this essential core kernel by ensuring communication between the FC nodes or network channels to the hypervisor and datacenters is provided via SSL.

5. Security Risk Profile

Based on observation of our evaluation of security offerings in Windows Azure, security of applications running and executed in the host/compute component and key management of storage access keys on the backend component appear more vulnerable. These components are considered to be of high and medium risks respectively. The vulnerability of the host/compute component is based on the type of security controls implemented on developed web based applications hosted on the cloud. Since developers have control on the management of applications deployed in the cloud, this determines how vulnerable the cloud service can be and also depends on proper security configuration of provisioned VMs.

A vulnerable application will enable an attacker access to the VM(s). On the other hand, a compromised VM exposes the Hyper-V (hypervisor) to security threats.

Table 3. Risk Log

Windows Azure Components	Taxonomy		Risk Level
Developer Environment	Identity Access Management	App Security Encryption/Key Mgt.	Low
Host/Compute Component	Application Security	Virtualization Security	High
Back End Component	Network Security	Data Security Encryption/Key Mgt.	Medium

Blue indicates security implemented by developer
Grey indicates security implemented by CSP

Table 3 shows that the host/compute component has a high risk level due to the application security management and implementation capabilities of the developer. The backend component is less vulnerable due to the complexity of breaking encryption on stored data and access to storage keys by an attacker. This is followed by the developer environment which has a low risk level due to identity and access management security implementation controlled solely by the CSP.

6. Conclusion

In this paper, we have been able to segregate Windows Azure into three components. This segregation enabled us understand how the components integrate to form the cloud and especially the security mechanisms implemented on each component of its architecture. We were able to use taxonomy of PaaS security to evaluate the cloud architecture and determine existing security mechanisms and controls that are implemented to meet industry security requirements.

In summary, most of the security techniques implemented on traditional information systems are prevalent on this type of cloud and much more provided through virtualization security to preserve the confidentiality, integrity and availability of information resources and assets hosted on the cloud. However, further research needs to be conducted through penetration tests to analyze how secure the platform is. The vulnerabilities from our evaluation strategy indicates that the security risks on PaaS components vary and more needs to be done by developers in building secure web/mobile applications to avoid the vulnerability that could be presented through compromised VMs and easy access to data storage keys.

7. References

[1] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V.3.0, 2011. Available at www.cloudsecurityalliance.org/guidance/csaguidev3.0.pdf

[2] A. Akinbi, E. Pereira, C. Beaumont, Identifying Security Methods and Controls for Secure PaaS Cloud Environments, 14th Annual PGnet Symposium 2012. Available at http://www.cms.livjm.ac.uk/pgnet2013/ Proceedings/papers/156 9757101.pdf

[3] A. Kumar, B.G. Lee, Secure Storage and Access of Data in Cloud Computing- International Conference on ICT Convergence (ICTC), 2012. Available at http://ieeexplore.ieee.org/

[4] NIST, Recommended Security Controls for Federal Information Systems and Organizations. http://csrc.nist.gov/publications, 2009

[5] M.T Sandikkaya, A.E. Harmanci, Security Problems of Platform-as-a-Service (PaaS) Clouds and Practical Solutions to the Problems, IEEE 31st Symposium on Reliable Distributed Systems (SRDS) 2012. Available at http://ieeexplore.ieee.org/

[6] Windows Azure App Fabric: Comprehensive Cloud

Middleware- online document available at download.microsoft.com/.../Windows-Azure-AppFabric-PDC10-Overview

[7] F. Sabahi, Cloud Computing Security Threats and Responses. IEEE 3rd International Conference on Communication Software and Networks (ICCSN), 2011 available at www.ieeeexplore.ieee.org

[8] B. P Rimal, E. Choi & I. Lumb A Taxonomy and Survey on Cloud Systems. Fifth International Joint Conference on NC, IMS and IDC, 2009. NCM 2009. Available at www.ieeeexplore.ieee.org

[9] C. Priya, N. Prabakaran Security Management in Inter-Cloud International Journal, 2012 - Available at www. ijettcs.org

[10] Towards Secure and Effective Utilization over Encrypted Cloud Data by Cong Wang ; Qian Wang ; Kui Ren Distributed Computing Systems Workshops (ICDCSW), 2011

[11] Security and Privacy Challenges in Cloud Computing Environments by Takabi, H.Security & Privacy, IEEE (Volume: 8 , Issue: 6)

[12] L. Yan, C. Rong and G. Zhao, Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-Based Cryptography, Cloud Com 2009, LNCS 5931, pp. 167-177, 2009. Springer-Verlang Berlin, Heidelberg 2009.

[13] M.R Islam, M. Habiba, Agent based framework for providing security to data storage in cloud", Computer and Information Technology (ICCIT), 2012 15th International Conference on, On page(s): 446 – 451

[14] M. Nabeel, N. Shang & E Bernito, Privacy Preserving Policy Based Content Sharing in Public Clouds- IEEE-available at www.ieeeexplore.ieee.org.

[15] Security of Cloud Computing Providers Study Sponsored by CA Technologies Independently conducted by Ponemon Institute LLC Publication Date: April 2011

[16] Encryption in the Cloud. Sponsored by Thales e-Security. 2012. Available at www.ponemon.com

[17] Windows Azure Fabric Overview documentation-available at www.microsoft.com.

[18] M. McKeown. Windows Azure blog, 2012. Available at www.michaelkeownblog.wordpress.org

[19] Eliminating the Hypervisor Attack Surface for a More Secure Cloud- Jakub Szefer, Eric Keller, Ruby B. Lee and Jennifer Rexford

[20] Differences Between the Storage Emulator and Windows Azure Storage Services- windows azure documentation 2012. www.microsoft.com

[21] C. Kaufman, R. Ventakapathy, Windows Azure Security Overview, 2010. Available at www.microsoft.com

[22] Windows Azure Documentation, 2012. Available at www.windowsazure.com

