Platform as a Service (PaaS) in Public Cloud: Challenges and Mitigating Strategy

Fidel Ikundi(✉), Rafiqul Islam, and Peter White

School of Computing and Mathematics,
Charles Sturt University, Bathurst, Australia
ikundif@yahoo.fr, {mislam,pewhite}@csu.edu.au

Abstract. Cloud computing is geared towards the effective and efficient use of computational resources and it has been making a big revolution in the field of information technology by reducing capital investment. It delivers computing as a service, that enables effective utilization of computational resources, rather than, a product, for a fraction of the cost. This paper explores key security issues associated with PaaS and proposed mitigating strategies are provided. These security challenges slow down the adoption of PaaS. Mitigating these security issues could increase PaaS adoption. This paper focuses on the security issues associated with Platform as a Service (PaaS) offering on a public cloud platform and provides various mitigating techniques to address these security issues. If properly implemented, we could realize an increase in PaaS adoption.

Keywords: PaaS · Cloud computing · Security

1 Introduction

Cloud computing is a concept that provides economic outsourcing of computational resources and qualified maintenance [8]. Various kinds of computational resources are shared through simple interfaces via high-capacity networks [12]. Despite the many benefits of cloud computing, such as better utilization of resources and less time taken in deploying new services, the sharing of resources in a PaaS platform has security challenges. These challenges range from access control issues to privacy awareness. Ubiquitously shared and distributed resources bring a new series of security problems that professionals in information technology need to address.

Eliminating this security challenges will speed up PaaS adoption and increase its usage. An increase in PaaS usage leads to better utilization of computational resources. It will also shorten time to deploy new services, speeds up technology adaptation, as well as carbon footprint [1].

Cloud computing has four deployment models [5]. These deployment models are:

- Public cloud – provides shared resources to a community of users
- Private cloud – provides services which are controlled and exclusive to the user
- Hybrid cloud – provides the ability to move workloads between private and public platforms

R. Deng et al. (Eds.): SecureComm 2016, LNICST 198, pp. 296–304, 2017.
DOI: 10.1007/978-3-319-59608-2_17

- Community cloud – provisioned for organizations with shared concerns Similarly, cloud computing has three service delivery models [5]. These models are:
- Software as a Service (SaaS) – consumed as a service only for the applications needed
- Platform as a Service (PaaS) – provides the core hosting operating system and optional building block services that allow users to run their own applications
- Infrastructure as a Service (IaaS) – outsource the elements of infrastructure like virtualization, storage, networking and load balancers.

PaaS plays a significant role in a cloud environment because it brings customs software development to the cloud. Moreover, PaaS provides an environment for users to run applications. Examples of PaaS services includes SharePoint or MSSQL server on Azure. PaaS is defined as "the capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider" [5]. PaaS will drive demand for cloud computing as desktop operating systems and development tools drove the demand for PCs in the 1990s. "PaaS consumers employ the tools and execution resources provided by cloud providers to develop, test, deploy and manage the operation of PaaS applications hosted in a cloud environment. PaaS consumers can be application developers who design and implement application software; application testers who run and test applications hosted in a cloud-based environment; or, application developers who publish applications into the cloud. PaaS consumers can be billed according to the number of PaaS users; the processing, storage and network resources consumed by the PaaS application; and the duration of the platform usage" [5].

PaaS is not a single technology. It is a collection of related services used in creating and deploying software on a cloud platform. PaaS brings challenges along with its many benefits, like all new technologies. Getting to PaaS success requires understanding what can get in the way of its fullest realization. While some PaaS challenges are organizational, others are technical in nature. However, these challenges do not exist in a vacuum. They exist in an organizational specific setting. Depending on an organizational potential PaaS users and choice of PaaS technology, they will encounter different types of the major PaaS challenges.

Concerns about cloud security are not new, however, PaaS could increase risk exposure. The cloud tends to blur the security perimeter in general because with PaaS, an organization's business extends to multi-tenant servers in unknown geographic locations. If a PaaS application connects to other enterprise systems, it could become a "route" for improper access and potential vulnerability. Connections between cloud-based applications built on PaaS and other enterprise systems present security, operational and governance challenges. The paas-based software is inherently service-oriented. It has the ability to call on application programming interfaces (APIs) exposed on numerous systems. These include APIs that use Simple Object Access Protocol (SOAP) as well as the increasingly popular Representational State Transfer (REST). Without adequate controls, systems can be exposed through APIs along with the business processes they support. Of course, few organizations simply leave an API totally open to the world. However, the difference in development and change cycles between legacy systems and PaaS software can lead to challenges because the legacy

system cannot keep up with new PaaS features. If external users can access internal business process through APIs that are out of sync, that can cause operational and compliance difficulties. Alternatively, if an API is not available because a change in the PaaS solution has broken the connection, that is also bad for business.

In this paper, we will focus on the key characteristics of a PaaS platform, security risks associated with a PaaS environment and proposed mitigation strategy.

2 Key Characteristics of PaaS

PaaS offering is widely being adopted in the business world; as a result, it is gaining rapid growth. This growth is bringing broad changes across the information technology sector. PaaS vendors are contemplating how to take the opportunity to this new expanding market and many developers are moving towards PaaS application development. Moreover, the increase in PaaS application consumption and development is driving the need for a platform technology built specifically to support the PaaS market. Below are some of the attributes behind the PaaS market expansion:

- **Multi-tenant architecture**

A PaaS platform has to be multi-tenanted. A multi-tenant platform is one that uses common computing resources including hardware, operating system, application code and a single underlying database with a shared schema to support multiple customers simultaneously.

- **Customizable/Programmable User Interface**

A PaaS platform must provide the capability to construct highly flexible user interfaces through a simple "drag & drop" methodology that permits the creation and configuration of UI components [2]. This "drag & drop" capability allows the creation of new layers quickly and easily without requiring much custom coding.

- **Unlimited Database Customizations**

The core of many applications is data persistence. Therefore, a key characteristic of PaaS is facilitating the creation, configuration, and deployment of persistent objects without requiring programming knowledge. So, a PaaS platform must have the capability to support the construction of objects, the definition of relationships between the objects and the configuration of advanced data behavior all from within the comfort of the Web browser via a "point and click" declarative concept.

- **Robust Workflow engine/capabilities**

The objective of a business process execution through process automation is vital to establish any business application in the business world. A PaaS offering should be able to offer a business-logic engine that can support the definition of workflow processes and the specification of business rules to engender process automation [8]. A workflow process defines the different stages a business object flows through, during its life cycle.

- **Granular control over security/sharing (permissions model)**

The PaaS offering should provide a flexible access control system that allows detailed control over what users of the SaaS application can see and the data each user can access. Definition of access from the application level (including tabs, menus, objects, views, charts, reports and workflow actions) to the individual field level should be possible. Defining an access control model should be possible through the creation of groups and roles and the assignment of users to groups or roles. For complex large-scale implementations, the ability to define which features and data each user can access should be available so users can be segmented across common organizational structures to provide fine-grained access to data/application features.

- **Flexible "services-enabled" integration model**

PaaS facilitates the rapid construction of applications in the cloud by providing foundational elements, such as data persistence and workflow capabilities that are essential to the creation of any business application. However, given the complex IT environments that permeate most enterprises today, the PaaS offering should leverage Service Oriented Architecture (SOA) principles to enable seamless integration of cloud application data and functionality residing in the cloud platform with other on-premise/on-demand systems and applications [8].

3 Challenges of PaaS

In the PaaS environment, the user objects are spread over the host. This could make it easier for objects to gain access to resources. In order to mitigate such risk, the objects will need to be protected from malicious providers.

PaaS is in a multi-tenant environment. This implies the environment is shared with other customers. Accessing a network in a shared environment brings challenges, such as access control and secure communication. However, access control and secure communication are not the only concerns in a multi-tenancy environment.

In the cloud environment, software and hardware resources from different vendors are integrated for efficient use. This integration of computing resources may bring about security challenges because the security setting of each computing resource may be different [12]. Similarly, each resource that is shared in a shared platform is a communication channel [11]. This could lead to a potential communication leakage.

Below are some of the challenges encountered in PaaS in a public cloud and strategies to mitigate the challenges.

- **Lack of interoperability**

The pooling of resources could eventually end up causing security vulnerabilities if access to the resources is not controlled. A security setting for a particular resource could lead to a breach to another. For example, Jones is authorized to access a file named "Passive" but mistakenly gained access to a secret file named "PASSIVE". "Interoperability can be maintained by providing common interfaces to objects for resource access" [8]. However, in order to control access to a PaaS platform, resource interfaces should be designed carefully.

- **Vulnerable hosts**

The idea of sharing the same platform in the cloud by multiple users has been around for a long time [6]. In recent times, this concept is still widely used. A multi-tenancy environment is made up of objects and hosts. These hosts and objects need protection.

However, if this protection fails, an attacker could gain access to both the resources of the hosts and tenant objects as well. This protection can be achieved by evaluating resource access request from each object on the host. TCB is a solution for hosts' vulnerability.

- **Vulnerable objects**

An object in a PaaS environment can either be compromised when a service provider accesses a user's object residing in the hosts, a user may attack another users' object in the same hosts or an attack by a third party. A service provider needs access to an object to execute the object. An object cannot be executed only when it is stored in the cloud.

- **Access control**

Access to remote entities must be controlled to keep network communication confidential. Some of the common attacks in a cloud-based environment are; phishing attacks, brute force attacks, and password reset attacks. Authentication, authorization, and traceability are the major concepts of access control. Solutions such as two-factor authentication (smart cards and biometric mechanisms) could protect against such attacks.

3.1 Proposed Mitigating Strategies

Lack of interoperability and vulnerable hosts can be mitigated by the use of trusted computing base (TCB). On the other hand, the risks posed by vulnerable objects can be mitigated by protecting the sensitive parts of the objects with encryption.

- TCB is a secure collection of executable code and configuration files. It is assumed to be secure because it is thoroughly analyzed for vulnerabilities before installing as a layer over the operating system. It provides standardized application programming interface (API) for the user objects. The principle of minimizing TCB is a widely accepted solution for a secure solution [6]. Interoperability is achieved when TCB is installed on every host and resource assignments are accessed via TCB. Every request assignment is checked by TCB, thus, preventing any possible attack from objects to hosts.
- Encrypting the objects to protect the integrity and privacy of a user object while the object is on the host is the responsibility of the service provider. The consumer trusts that the objects are protected. However, if a host is breached or the provider is malicious, the object could be read, rendered inaccessible, modified or deleted. Symmetric and asymmetric encryption schemes, hashing and signatures could be used to protect the content in an object. This could prevent the content in an object

from being accessed. Key storage is very important in a PaaS environment in a public cloud. Users' keys should be stored in an encapsulated key storage field according to their access roles. Encryption should be applied on the keys themselves for added security (Tables 1 and 2).

Table 1. Challenges and solutions to breaching an object's security.

Challenge	Proposed solution
Lack of interoperability	Use trusted computing base (TCB)
Vulnerable host	Use TCB
Vulnerable object	Encrypt objects Use hashing schemes Use signatures Implement access controls policies encrypt key storage

Table 2. Network access challenges and proposed solution

Network challenge	Proposed solution
Confidentiality	• Use transport layer security (TLS) • Implement access control policies
Authentication	• Use TLS • Implement access control policies
Authorization	• Use policy enforcement points (PEPs) • Implement access control policies
Traceability	• Keep records of events • Users should monitor their applications • Users should audit their data

3.2 Broad Network Access and Measured Services Challenges

There are some basic requirements for securing a network communication. The confidentiality of communications over a network channel must be guaranteed and remote users must be authenticated for a secure network access. Authentication, authorization, confidentiality, and traceability are the backbone of access control.

- **Authentication**

This is a process in which credentials are compared with what is stored on file during an interaction. Authentication is a method of identifying who is requesting or attempting access.

- **Authorization**

Authorization is the method of granting access to specified resources. This is another form of access control. When attempting to gain access to an object in a PaaS environment, authorization will definitely allow only the authenticated individual with the correct authorization to access the object. The object will be compromised if

authorization mechanisms are not in place. Objects in a PaaS public cloud are not stable. They are constantly migrating and the host could also be reconfigured, it may be possible that a reconfiguration may change or degrade the access policy.

In a PaaS environment, hosts are very intelligent because they have to know each object's specific policy. This will enable the host to apply the specific policy to an individual object.

- **Confidentiality**

The notion that communication over a network channel needs to be confidential is one of the most important roles of a network security professional. In a PaaS platform, the users will need to communicate with the objects. This communication could be intercepted and sensitive information could be stolen from the host. As a result, it is vital to implement security in the communication.

- **Traceability**

This access control method can be realized by keeping records of all occurrences on the platform. The stakeholder in the cloud would like to know what is actually going on. Stakeholders are actually billed on usage, so as a result, they will like to monitor and audit any access to their data. These records are actually kept in logging systems. These systems should be protected and secured.

3.2.1 Proposed Mitigating Strategies

By using a transport layer security (TLS) we can achieve access control mechanisms in a PaaS environment. Access control policies can be enclosed in similar objects. This will enable an easy distribution and customization. "Authorization is applied on the hosts with the help of policy enforcement points (PEPs) with respect to the encapsulated access control policies" [10]. To trace events that happen in the cloud environment, a logging protocol is introduced.

- **Transport Layer Security (TLS)**

Confidential channels can be formed through TLS to prevent eavesdropping and for secure authentication [11]. While the object is being accessed, it is recommended to have mutual authentication in place, so as to avoid a man-in-the-middle attack [9].

- **Policy Enforcement Points (PEPs)**

PEP is software used to read and manage the encapsulated access control policies embedded in the objects. During the decision-making process, PEPs of the host must behave according to the undeniable logging protocol [10]. PEPs are normally tied to the hosts. The PEP will read the object's access control policies and consequently decides if the connection will be established.

- **Undeniable Logging Protocol**

In this protocol, malicious activities are detected and exposed to the parties concerned. This protocol helps in investigating incidents that occur in a PaaS environment in the public cloud. There is an online bulletin board that helps to ensure that the logs cached by this protocol have not been tampered with. The bulletin board is a public

write-only storage. If a related party needs access, they will send an access request. However, the request is not sent directly to the related party but through the bulletin board. So the bulletin board logs the activities of both parties.

4 Privacy Awareness Challenges

For a user to be authenticated, the user will need to provide very specific information. For example, if an employee of a company wants to access the company's printer, using his or her personal laptop, the printer will refuse access.

However, if the employee is using a work laptop, access will be granted. When accessing devices or materials through the Internet, users should be careful not to provide too much information because their privacy may be compromised [13]. Proxy certificates can help to reduce the risk of revealing excess attributes [7]. When using privacy aware authentication with a proxy certificate, the following will need to be met:

- More attributes must not be requested by the host and the object than the attributes that they need. "If more attributes than required is requested, the only practical solution is negotiating the service terms" [7].
- With the assistance of a trusted third party, the credentials should be easy to configure.

5 Service Continuity and Fault-Tolerance Challenges

Service interruption is not new in a networked platform. Attacks such as distributed denial of service (DDoS) can compromise the systems in a network and makes the network stop. If there are any network issues in a PaaS environment, the contents of the objects may be modified or even completely wiped out by a malicious attacker. "Byzantine quorum approach is adopted to obtain fault-tolerance and service continuity under these circumstances" [4]. In the Byzantine quorum approach, "any subset of all hosts that resides the copies of the same object forms a quorum" [3]. We can determine a copy of the object where the number of hosts is enough. As a result of that, in the byzantine quorum system, any modification of the object will be detected.

6 Conclusion

PaaS technologies have the potential to accelerate software development while reinventing how IT supports the development process. With PaaS, developers are tempted to take shortcuts and release applications without considering important security factors. There has to be a balance between the need for speed and sensible planning and controls. Many software tools are available to coordinate and control the PaaS development process. PaaS success is an organizational issue. However, the technology itself can only do so much to bring about the kind of collaboration that will make PaaS an effective mode of software development. However, PaaS infrastructure will deliver

best results when security challenges are understood and mitigation strategies implemented. Moreover, operational plans have to align with security.

In this paper, we have designed some strategies in which a PaaS offering in the public cloud could be rendered secure. Some security challenges, such as resource pooling and rapid elasticity, broadband network access and measured services, privacy awareness issues, service continuity and fault-tolerance challenges have been investigated and proposed strategies to mitigate the above security challenges discussed.

References

1. Brunette, G.: Platform as a service offering. J. Cloud Comput. **10**(3), 17–21 (2015)
2. Dijk, M., Juels, A.: Attributes of platform as a service offering. J. Cloud Comput. **17**(4), 20–23 (2015)
3. Gallagher, M.: Understanding platform as a service models. J. Inf. Technol. **18**(4), 33–37 (2015)
4. Kaufmann, M.: Data security in the world of cloud computing. J. Secur. Priv. **9**(2), 54–63 (2015)
5. Mell, P., Grance, T.: The NIST definition of cloud computing. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf. Accessed 25 Mar 2016
6. Momm, C.: The principle of minimizing TCB (2014). https://mommconrad.com/threats/multitenancyplatformsv1.0.pdf. Accessed 21 Mar 2016
7. Natis, Y.: Research on platform as a service. J. Cloud Comput. Secur. **10**(1), 11–16 (2015)
8. Osvik, D., Shamir, A.: The concept of cloud computing. J. Inf. Technol. **12**(3), 26–29 (2015)
9. Percival, C.: Securing the transport layer. p. 25. The New York Times. http://www.nytimes.com. Accessed 20 Jan 2015
10. Saltzer, J.: Protection and the control of information sharing. In: ACM Conference on Information Sharing and Protection, vol. 6, no. 2, pp. 11–15 (2014)
11. Shacham, H., Savage, S.: Exploring information leakage in third-party commute clouds. J. Cloud Comput. **9**(1), 13–17 (2015)
12. Subashini, S., Kavitha, V.: Shared resources in the cloud. J. Netw. Comput. Appl. **14**(2), 27–29 (2015)
13. Takabi, H., Joshi, D.: Security and privacy challenge in cloud computing environments. J. Cloud Comput. Secur. **23**(1), 66–72 (2015)