

## ► PaaS Threats In The Cloud

---

Tech Tip  
by Philip Cox

© Copyright 2010 SystemExperts Corporation. All rights reserved.

## ► PaaS Threats In The Cloud

---

### What are the likely threats in a Public PaaS Cloud offering?

Following on my last Tech Tip, we'll focus on the top Platform as a Service (PaaS) threats you are likely to encounter. In the SaaS model, the consumer was a user, and relied on the provider to secure the application. In PaaS, control (and security) of the application is moved to the consumer, and the provider secures the underlying cloud infrastructure (i.e., firewalls, servers, operating systems, etc). Like last time, we'll talk about the threats you can do something about, not those that you rely on your provider to take care of.

### What are the most likely threats in a PaaS Cloud service?

From my experience here are the most likely threats you'll have to deal with in a Cloud based Platform as a Service (SaaS) offering:

- › Default Application Configurations
- › SSL protocol and implementation flaws
- › Insecure permissions on Cloud data

While there are many more other risks and vulnerabilities, I feel the ones listed above are the most likely to affect you and your deployment in a very real manner. Remember that the threats to SaaS we discussed last time are still applicable, and must be mitigated.

#### Default Application Configurations

You will be running an application on the Cloud infrastructure, and the likelihood that the application is secure in its default configuration is probably zero. Thus, making changes to the default application installation will be the number one security mitigation that you will perform. You will need to be familiar with the security configuration of the following applications (i.e., you need to know how to secure them if you use them), as they make up

roughly 80% of all applications that exist in the Cloud:

- › LAMP: In the LAMP<sup>1</sup> stack, the Apache, MySQL, and PHP will require your focus and expertise.
- › Windows: In a Windows environment, you will need the ability to secure IIS, Microsoft SQL, and .NET (basically a Windows LAMP equivalent).

As far as practical mitigation steps for the above items, the three top things to look for are:

- › Default and sample files and directories left after installation.
- › Excessive services offered, such as WebDAV, FrontPage, LDAP, SNMP, etc.
- › Default usernames and passwords for application administration (usually Web or SNMP).

Other than those, you should go to the specific vendor site for security configuration recommendations.

#### SSL protocol and implementation flaws

The second greatest threat to PaaS consumers will be SSL based attacks. SSL is the underpinnings of most of the "security" utilized in the Cloud or for that matter the Internet in general. The current focus of the hacking community on breaking SSL will become a major exploit vector in the near future. Understanding this and taking all possible steps to mitigate attacks on SSL must be secondary only to making sure the applications are not open to default attacks.

To give you some scope of the problem, in November 2009 a protocol level bug in SSL that opened up a number of man-in-the-middle (MITM) attacks related to renegotiation. Since this is a flaw in the protocol, any implementation that was based on the protocol has to be patched. Another occurrence early last summer, showed how to spoof an SSL certificate by adding a "null" string character to the certificate fields, and subsequently

---

<sup>1</sup> A common configuration based on Linux, Apache, MySQL, and PHP.

## ▶ PaaS Threats In The Cloud

---

fooling the client into thinking it was talking to the real server. These are just a couple of the recent research on SSL. There will be more, and you will need to be diligent.

As far as mitigating these threats, they will be very implementation specific, and you will rely on the application vendor to provide details of how to apply the correct configuration/patches in a timely manner. Timeliness is critical here; make sure you have a change management program that will allow patches and changes to SSL to occur in a very rapid manner.

### Insecure permissions on Cloud data

The third major threat that you will need to address as a PaaS consumer is proper permission on the data you have stored in the Cloud. While this may seem like a given, many of the applications that I have performed security testing on have had serious information leakage because the underlying permissions on the data were not set correctly. From a security standpoint, this means that there was too much access, not too little, granted.

The mitigation for this threat is twofold: Design your application to use granular security, and ensure all users of the application are required to authenticate prior to using the application. This way, you can apply appropriate permissions to the data, and the application can make access control decisions based on user authentication.

## Closing Thoughts

We have addressed the top three “real” threats as I see them in a Public Cloud PaaS offering. Do these things:

- ▶ Properly secure the application, using vendor suggestions applied to you specific implementation.
- ▶ Have the ability to deal with SSL issues in a very quick and agile manner.
- ▶ Assign user accounts and apply appropriate access permissions based on the user/role.

And you will be very effective in making your PaaS secure.

One last item, I cannot overstate my concern over the SSL based issues that will be surfacing over the next year or so. Do not underestimate the depth and extensiveness of the problem.

## Author Information

Philip Cox  
CISSP, CISM, PCI QSA, NSA IAM/IEM  
Principle Consultant  
SystemExperts Corporation  
Email: phil.cox@systemexperts.com  
Phone: (530) 887-9251