Vulnerabilities in SaaS Layer of Cloud Computing

Clinton D Souza, cvdsouza@asu.edu, **Rafael Santana,** rsantana@asu.edu, **Dr. Partha Dasgupta** partha@asu.edu

School of Computing, Informatics, Decision and Systems Engineering
Arizona State University,
Tempe, AZ, USA

Abstract

Cloud computing services are being leveraged to a great extent in the industry today, extensive research is being conducted by multi-national companies on its integration into their infrastructure, and services are being implemented to as to make data and applications available to customers from anywhere around the world with access to the internet. However with the rise in popularity of this service, customers and clients have raised concerns on the security, authenticity, and availability of services, which they are paying for either individually or for an organization. These concerns further intensify when services are made available in the public cloud infrastructure, using the Software as a Service (SaaS) layer of cloud computing. The public cloud infrastructure is designed such that authorized access is not limited to a closed group or organization but to the general public, which may include malicious users. Software applications in the SaaS layer in this infrastructure are at a greater risk of exploitation due to its ease of access and availability of the service. This research aims to identify the vulnerabilities in the SaaS layer of the cloud model, which will help to not only raise awareness of the current vulnerabilities existent in the cloud model, but will also help to identify future risks which could compromise user data.

Introduction

The basic structure of the cloud computing architecture is divided into three layers: Infrastructure as a Service (IaaS), Platform as a Service (Paas) and Software as a Service (SaaS). IaaS provides the basic computing resources to host a services, for example server infrastructure, virtual machines, firewall, Virtual LANs. PaaS [1] facilitates deployment of services and provides tools to develop an application service including the OS platform. SaaS is a software distribution model in which the applications are hosted by the vendor and made available to the customer over a network either through a web or mobile interface.

The cloud computing industry has developed extensively and services, platforms and infrastructures are being offered to multi-national companies to host both private as well as public applications and services for clients and customers. However with companies moving applications to the cloud (such as Amazon EC2, AT&T, Cisco, EMC, Cloudscale), there comes an issue of privacy, identity management, network security, data security and access control. These issues intensify when services are loaded on a public cloud infrastructure and are being hosted on a SaaS layer by third party vendors. Poor understanding of the basic foundation of cloud models, and unawareness towards the current

vulnerabilities and mitigation strategies are preventing large multi-national companies from moving resources to the cloud.

In the SaaS service model, the cloud provider installs operational and functioning application software in the cloud, which users can access through client portals. The cloud users do not manage the cloud infrastructure and platform on which the application is running.

Our research goal was to determine the most important attack points, also known as *points of entry*, into a SaaS service model, and the types of attacks that a malicious user can launch by exploiting these entry points. Since this model is being widely considered by companies to provide efficient access to clients from all around the world to generate more income and clientele, we believe that by focusing of the SaaS layer we will be able to address concerns and prove the weak points that are present on the software as a service layer of cloud computing.

We studied the architecture of the SaaS layer of the model, inclusive of its detailed structure and framework. We attempted to determine the malicious points of entry into this layer and how these points can be further exploited. We studied the different kinds of attacks that usually occur on regular web-services and databases, and show through examples and theory how these attacks can be carried to the cloud, if proper data policies and access control is not maintained in the cloud.

Results and Discussions

In our research to find the most vulnerable attack points in Software as a Service model (SaaS), we found that there are two main points of entry into this service.

(i) User Point of Entry
(ii) Provider Point of Entry [2].

Of the two, the user point of entry is the most common point of attack in a SaaS model. The main reason being that, like every browser and application online, for a user to connect to the uploaded SaaS application, he will have to use a client/user portal which uses a web service interface that is vulnerable to a variety of attacks, some of which include, buffer overflow, SQL injection, Cross Site scripting and Denial of Service [2]. Based on Verizon's 2012 Data Breach Investigation Report, SQL injection ranks 5th, in single action breaches by an attacker [3]. An example query that exploits the vulnerability in most database servers like PostgresSQL and MySQL, which will grant the attacker administrator privileges could be [4]:

'%admin% to *$uid* to change the admin's password, or simply sets *$pwd* to ***hehehe', trusted=100, admin='yes***

```php
<?php

// $uid: ' or uid like '%admin%
$query = "UPDATE usertable SET pwd='...' WHERE uid='' or uid like '%admin
%';";

// $pwd: hehehe', trusted=100, admin='yes
$query = "UPDATE usertable SET pwd='hehehe', trusted=100, admin='yes' WHE
RE
...;";

?>
```

Figure 1. PHP SQL query injection

Another possible query for execution with PHP could be as shown in Figure 1 (note that the figure *contains only example code, and may not work if executed, as servers should already have security measures implemented (such as parameterized inputs).*

The model in Figure 2 below is a consolidation of the most common attacks possible associated with SaaS model in a public cloud infrastructure. They are divided into the following four groups: Availability, Data Security, Network Security and Identity Management.

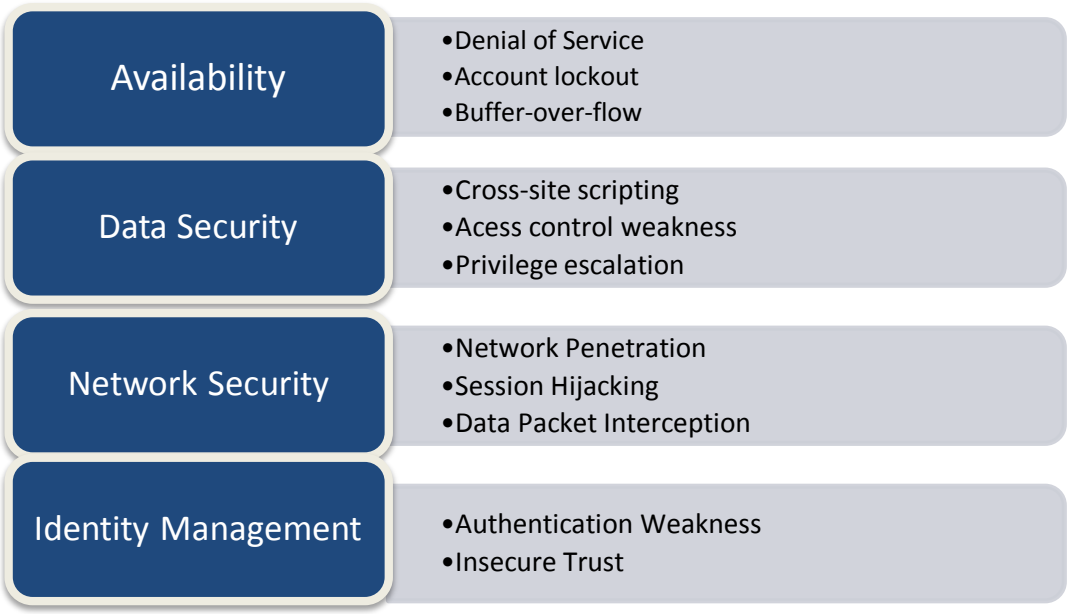

Figure 2. SaaS (Software as a Service) vulnerabilities

An attack on a web service using techniques such as SQL injection attacks or Cross-Site-Scripting attacks not only compromises a the web service, but also the database containing sensitive data of both the users as well as the providers.

While researching on these attacks, and their impact on the software service and their applications, we looked for possible solutions that have already been implemented, although solutions

provided by HP, and IBM have proved to be effective, crackers are still able to hack into these security solutions.

Two recent incidents proved that security suites are not the most effective means of prevention of attacks in a SaaS model:

(i) Panda Security hacked by Antisec
(ii) Zero-Day Vulnerability Found in McAfee's SaaS Products

Conclusion

There are many advantages when it comes to using a cloud computing model but despite those advantages various vulnerabilities are encountered in this new technology. In this paper we discuss the vulnerabilities found at the SaaS layer, which after thoroughly analyzing this cloud-computing layer, we were able to construct a model associating each factor crucial in a SaaS model to its corresponding attack. Additionally we were also able to find security incidents, which proved that security suites are not completely secure since they themselves can be exploited.

Finally we found two main attack points through which access can be attained in the SaaS model. The most common of these were the User point of entry due to the fact that thousands of users can access a single software application at any given time, thus making that point of entry more susceptible to attacks from malicious users.

Acknowledgments

I would like to express my gratitude to the FURI (Fulton Undergraduate Research Initiative) program at Arizona State University for providing the opportunity to work on this cutting-edge research topic at such an early stage in our careers. The encouragement and support provided was invaluable.

References:

[1] GoGrid Cloud Hosting, "*Cloud Infrastructure"*, http://pyramid.gogrid.com/#/, 2010

[2] Tipton,Harold F. ; Nozaki, Micki Krause , *Information Security Management Handbook*. 6th ed. USA: CRS Press. 2012

[3] Verizon Bussiness, *"2012 Data Breach Investigations Report"* http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf, 2012

[4] The PHP Group,"*SQL Injection",* http://php.net/manual/en/security.database.sql-injection.php, 2001-2012