COS700 Research Project

Tjaart Bester

October 2, 2014

1 Abstract:

Cloud computing offers benefits such as high availability, on demand access from anywhere on any device at any time, cost saving, scalability etc. Security concerns have been cited as one of the biggest challenges to this new paradigm. Clarification of these security concerns will help identify real security risks which in turn will help decision maker make more informed decisions about cloud computing. In this paper I look into adding risk-based authentication to a public cloud.

2 Introduction:

The increased availability of computing resources in conjunction with the success of the internet has put the cloud computing paradigm at the cutting edge of a digital revolution. Cloud computing offers benefits such as high availability, on demand access from anywhere on any device at any time, cost saving, scalability etc. [2] Cloud computing also offers a new business model that outsources computing resources to a shared third party infrastructure.

Cloud computing resources may be clustered to offer public, private or hybrid networks. Private cloud: also known as internal or corporate cloud. A Private cloud is infrastructure created for a single entity but managed by a third party cloud service provider. Public cloud: is open to the general public over the internet on a pay-per-usage system. Placing systems and sensitive information into a public cloud in the middle of a hostile and open network (the internet) is seen as a risk that most companies are unwilling to take. Hybrid cloud: is a combination of atleast one public and one private

cloud.[1]

Cloud computing services can be classified into infrastructure as a service (IAAS), platform as a service (PAAS) and software as a service (SAAS). Delivering infrastructure, platforms or software as a service requires a high level of virtualisation and implementation of virtual machines. Virtual machines are created, clustered together and operated via a hypervisor. A hypervisor or virtual machine monitor creates a virtual platform for virtual machines and manages their execute.

Cloud computing offers resources and services to users regardless of physical or geographical boundaries at any time of day or night. For example a pharmaceutical company may move their stock control and manufacturing scheduling systems to a public cloud. This will give their sales representatives across the world access to current stock levels and production schedules in real time. The move to cloud computing will allow greater monitoring and improvement to the company's logistical infrastructure. But the information contained within this system would also be very valuable to competitors trying to secure a competitive edge in the market. Securing such a system with in a public cloud requires more than single factor authentication. Risk-based authentication is non-static authentication system that assigns a certain risk profile to each authentication attempt. The risk profile determines the complexity of the challenge. A High risk profile requires a strong challenge and a low risk profile can require as little as user name and password.

The following section we will look at motivation.

3 Motivation:

Authentication on the cloud can be improved by implementing a risk profile for each authentication attempt. For example logging in from your work computer in business hours is a lower risk than logging in from an unknown mobile device in different country in the middle of the night. With a low risk authentication attempt, a normal user name and password will suffice but as the risk increases so does the difficulty of the challenge for example a one time pin, supervisor authorization etc.

The low adoption rate of public clouds indicates that the business world is hesitant to make the move to cloud computing due to perceived security

challenges and vulnerabilities. There is a need for cloud computing authentication to be improved and to assure prospective user that cloud computing can give them the competitive edge without unnecessary risk to there business.
The following section we will look at the problem.

4 Problem:

The usage of mobile devices within the cloud computing is set to rise, even within corporate environments with the adoption of BYOD (bring you own device). Combined with the increase of different cloud services supplied by a myriad of service providers, has highlighted the need for a federated identity management with single sign-on service.

How to construct a federated identity management service to be used with cloud computing risk-based authentication?

The following section we will look at objectives.

5 Objectives

Investigate how device identification can be incorporated into user and system authentication within the cloud.
Investigate measures to improve user and system authentication on the cloud.

6 Related works

A. Cecil Donald[**?**] proposes a novel authentication mechanism to enhance security in the cloud environment. The use of a trusted authority that creates a digital signature to compare with the users created digital signature when services are requested from a cloud service provider.

L.F.B Soares[**?**] suggests a model where a proxy VM is placed between inbound connections and cloud management interfaces.

Richard Chow[**?**] proposes a novel authentication framework for mobile devices to cloud services. Where the recent history and activity is used to determine the appropriate level of authentication required.

7 Prototype

The prototype uses Xenserver for a hypervisor to supply the platform resource of a public PAAS cloud solution. Access to the cloud is controlled by a vnc-gateway server that send SAML2 authentication assertions to a IDP (WSO2 Identity server). The authentication assertion contains information gather from the connection devise (gps co-ordinates, trace route, etc.) to be compared with a risk profile for the user account.

References

[1] Cyril Onwubiko. Cloud Computing. pages 271–288, 2010.

[2] Qi Zhang, Lu Cheng, and Raouf Boutaba. Cloud computing: state-of-the-art and research challenges. *Journal of Internet Services and Applications*, 1(1):7–18, April 2010.