COS700 Research Project

Tjaart Bester

April 22, 2014

1 Abstract:

Cloud computing is a new paradigm that offers a wide variety of benefits such as high availability, access from anywhere on any device at any time, resources on demand, cost saving, etc. Security concerns have been cited as one of the biggest challenges to this new paradigm. Clarification of these security concerns will help remove sensationalism and identify real security risks which in turn will help decision maker make more informed decisions about cloud computing.

2 Introduction:

Cloud computing is a new paradigm that offers a wide variety of benefits such as high availability, access from anywhere on any device at any time, resources on demand, cost saving, etc. Cloud computing delivers Infrastructure, platform and software as a service (IAAS, PAAS, SAAS). These cloud services may be offered in public, private or hybrid network. Delivering infrastructure, platforms or software as a service requires a very high level of virtualisation, thus removing the physical separation which served to reinforced security and authentication in other paradigms. Placing systems, sensitive and critical 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.

3 Motivation:

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 companys 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. Ensuring that this information is only accessible to the authorized parties is hampered by the high use of virtualisation with the cloud paradigm, competing companies systems and information might reside next to each other within the cloud. This possible proximity and removal of physical separation has raised the requirement to ensuring effective and adequate user authentication. Delivering an authentication model to match the potential of the cloud will make the new paradigm more attractive to companies and businesses.

4 Problem:

Taking a look at traditional paradigms in authentication for public or hosted services/resources we see a reliance on physical separation and access only allowed through a fortified proxy. With cloud computing the hosted system or service is no longer within the confines of a companys local network but located in the cloud. Thus we see the need for effective and adequate authentication for resources, information and systems of varying importance within the public cloud is required. How to implement authentication for device independent paradigm such as Cloud Computing?

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.