Chapter 40
The University Library Electronic Identities Authentication System (UL-EIDA): Enhanced by Segmented Virtual Machines and VLANs for Deployment in the Sub-Saharan Region

Jameson Mbale
University of Namibia, Namibia

ABSTRACT

World-wide electronic university libraries, with wide accessibility, are considered to be essential units in both academic and nonacademic information utilization. Within this context, the developed world wasted no time improving and expanding their libraries by applying the technology leverage offered by cloud computing. As institutions from developed countries expanded the use of cloud technology for library applications, it became clear that this technology was highly vulnerable to security threats. Nevertheless, this did not retard advanced nations from proceeding. Undaunted, they forged ahead and now are busy building appropriate cloud computing security infrastructures. Despite progress in this area, very little has been done to expand the university libraries in the sub-Saharan region using cloud computing technologies. Even less has been done in these developing countries to plan and develop the building of library computing security infrastructures. It was in view of this deficit that the University of Namibia's (UNAM) University Library electronic Identities Authentication (UL-eIDA) system was conceived to build a cloud computing security framework model suitable for the sub-Saharan region.

INTRODUCTION

The University Library electronic Identities Authentication (UL-eIDA) system was initiated as a cloud computing security framework model suitable for use in the sub-Saharan region. The system was built upon three operational layers: traditional, interface, and the cloud environment. In this work the terms "layers" and "environment" will be used interchangeably. These layers were

DOI: 10.4018/978-1-4666-6539-2.ch040

then connected to the Cloud Provider which was subcontracted to acquire, provide and service the hardware and software.

The traditional layer consisted of: the University Library, UL-eIDA smart card authentication infrastructure, hardware firewall, server, and switch. The interface layer was composed of the VM/VLAN-Student, VM/VLAN-Staff, VM/VLAN-Community and generic firewalls. The cloud environment had the dynamic security zone (DSZ), and was divided into segmented VM/VLAN-Student, VM/VLAN-Staff, and VM/VLAN-Community networks.

The system was divided into three operational parts to support the conformity of data as it was processed in different environments. For instance, raw data could be processed in the traditional layer but not in cloud environment hence reformatting would be necessary. The data and equipment were virtualized to allow dynamic scaling of library applications. Boss, Malladi, Quan, Legregni, and Hall (2007) stated that by means of virtualization, the cloud is a pool of virtualized computer resources which allowed the dynamic scaling of applications abetted by the provisioning and de-provisioning of resources. In addition, the system was configured into three VLANs: VLAN-Student, VLAN-Staff, VLAN-Community networks. The VLANs provided a form of virtual isolation which constrained a group of users to limit their focus and efforts only to their networks. This provided security in the sense that it inhibited malicious intruders from crossing into other networks and domains to purposely destroy data.

The system uses the UL-eIDA, a smart card authentication infrastructure for strong authentication. With this technology, the user was authenticated once and got access to different networks without need for re-authentication. This is also known as "single sign on" technology, or merely SSO.

To further ensure that security was strong, the following measures were taken: first, the hardware firewall was installed and was used to filter data to-and-from the University library and interface layer. Second, a series of generic firewalls that filtered data to-and-from traditional and cloud environments. Third was the dynamic trust zone (DTZ) which was an assortment of security tools such as robust anti-virus software that screened and discarded all possible malicious malware.

The system employed the DFUL-eIDA Encryption infrastructure which was based upon the Delffi-Hellman algorithm (Forouzan, 2007). To conceal important information from intruders and hackers the DFUL-eIDA Encryption method applied mathematical principles where a symmetric key is used to both encrypt and decrypt messages. It was designed to work over an insecure public network. In a nutshell, a symmetric key might exist on the sender's system. Then certain information is then shared between the sender and receiver which allow the recipient to generate the same symmetric key allowing secure communications to proceed without having to ever exchange the symmetric or private key over the vulnerable network. This infrastructure is somewhat different than other more modern public key infrastructures which may use asymmetric keys whereby a private key is used to solely decrypt messages and a related public is only used to encrypt messages. The public key is transmitted or distributed between senders and receivers but the private key, which is used to decrypt messages and thus obtain information, is never exchanged between participants. In either method, intruders and hackers are completely deprived of private key access, which would be crucial for any breach of security.

The above security measures will be discussed in detail in later sections. However, the overview of security measures above should highlight how dynamic and robust the system is.

Statement of the Problem

Like any other universities worldwide, libraries are key elements in providing both academic and non-academic information to a range of subscribers.