Cross-domain Identity Management System for Cloud Environments

By
Umme Habiba
2010-NUST-MS-CCS-027

Supervisor
Dr. Muhammad Awais Shibli
Department of Computing

A thesis submitted in partial fulfillment of the requirements for the degree of Masters in Computer and Communication Security (MS CCS)

In
School of Electrical Engineering and Computer Science,
National University of Sciences and Technology (NUST),
Islamabad, Pakistan.

(February, 2014)

Abstract

Secure handling and sharing of Identity credentials across multiple domains is considered to be the gravest issue faced by Cloud service consumers and Cloud service providers. Identity credentials are generally considered to be the most sensitive information since its unauthorized disclosure may lead to many serious consequences. As a result, many efforts from academia (research community) and IT industry are underway to circumvent the misuse of identity information. Despite hundreds of thousands of scientific reports and books published on this domain, the issues related to identity management systems continue to grow in severity and sophistication. Apart from this, identity management systems have actively followed the evolution of technology which in turn has made their security and functionality requirements even more diverse and dynamic. The immediate result of this continuous arms race is that the domain of identity management has become quite complex. This complexity is two-fold. Firstly, the massive literature on identity management remains largely unstructured. Secondly, a cross-domain identity management system capable enough to ensure secure management of user credentials across multiple domains is sorely missing.

In this thesis, we explore and address the abovementioned issues by first structuring the knowledge in the domain of identity management in the form of a well-organized taxonomy, and then by implementing a cross-domain identity management system for Cloud. Comprehensive list of attacks that are targeted towards identity or identity management systems along with a taxonomy covering most eminent features and corresponding mechanisms to avoid those attacks are presented. It is asserted that the proposed taxonomy helps in making informed decisions while selecting or implementing a cross domain identity management system for Cloud environment. Further, System for Cross-domain Identity Management (SCIM) - an open source, extensible and light-weight protocol for the exchange of identity credentials among disparate identity management systems is explored and implemented. In addition to this, we have enhanced SCIM protocol by adding an encryption module that help ensures the confidentiality of identity credentials during

transmission across multiple service providers.

We have rigorously evaluated our work from two perspectives, functionality of the proposed system is certified through user defined test-cases and for security analysis we have chosen Scyther, a security protocol evaluation tool. The results of our evaluation confirm that there is significant enhancement in the functionality and security of SCIM protocol.