Interoperability among Access Control Models

By
Khalid Hafeez
2009-NUST-MS-PhD IT-16

Supervisor
Dr.Awais Shibli
Department of Computing

A thesis submitted in partial fulfillment of the requirements for the degree of Masters of Science in Information Technology (MS IT)

In

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

(February 2013)

Abstract

In the era of distributed computing and multi-user environment, federated organizations though running in isolation with their own proprietary identity stores, need to collaborate and access each other's resources. Each of them has to authenticate its self to get authorization for the utilization of desired resources. Organizations use their own identity stores with user's credentials and policy enforcement mechanism for authorizing user access to their resources. In order to access resources of different organizations, a user must have login for all of them. This requires multiple identities for the same user which is very complex and difficult to manage. These conditions become even worse if collaborating organizations have used heterogeneous access control models for implementing their authorization policies. Existing centralized solutions such as Single Sign On (SSO) suffers with single point of failure and single central server could result in performance bottlenecks if not handled properly. Other distributed solutions for collaborating organizations require major infrastructure change and they also require homogenous access control model to be used between two collaborating organizations. In order to access resources user must be authenticated seamlessly and authorized to perform access request.

This research has proposed a plugin based distributed solution by making access control models, existing in different organizations, interoperable. The proposed solution has shown how decentralized and distributed yet federated organizations with heterogeneous access control models can share valuable resources/services in a secure, reliable and efficient manner with no or minimal changes to their existing infrastructure. The proposed solution converts the existing policies of collaborating organizations into Attribute Based Access Control Model (ABAC) by a Model Transformation Utility (MTU). When our proposed system is plugged-in to existing Role Based Access Control (RBAC) system, MTU reads RBAC policies form legacy repository and transforms them to ABAC policies using Extensible Access Control Markup Language (XACML) and stores them into ABAC policies repository. These

policies are applied to remote request to obtain access over local resources.

In order to check the correctness of RBAC model transformation into ABAC model using XACML, a significant number of test cases have been designed, and executed on existing as well as transformed systems and the results comparison shows that model transformation is 100% correct.