Chapter XXXIII
Supporting Collaboration with Trust Virtual Organization

Aizhong Lin
Macquarie University, Australia

Erik Vullings
TNO, The Netherlands

James Dalziel
Macquarie University, Australia

ABSTRACT

This chapter introduces the trust virtual organization as a means of facilitating authentication and authorization for sharing distributed and protected contents and services. It indicates that sharing institutional protected services and deliverables has proven a hurdle since user accounts are created in many sites. It provides an approach to solving this problem using virtual organizations with cross-institutional Single Sign On, with which users use their existing institutional accounts to login. This chapter also presents the challenges of building trust virtual organizations: managing users from distributed identity providers; managing services from distributed service providers; managing trust relationships between users and services, and authorizing the access privileges to users based on the trust relationships. It argues that the trust virtual organization increase the effectiveness of e-learning, e-research and e-business significantly. Furthermore, the authors hope that the trust virtual organization facilitates not only Web-based authentication and authorization, but also grid-based authentication and authorization.

INTRODUCTION

Complex problems often require multi-disciplinary collaborations. The benefits of collaborations across organizations include (Kürümlüoglu, Nøstdal, & Karvonen, 2004): sharing knowledge, resources, and services among partners; reducing development time to market; spreading costs and risks with partners; accessing to new markets through partnerships; improving capacity utilization, and gaining access to global networks. Virtual organizations (VOs) are the new paradigms to support collaborations among semi-independent partners using communication tools and information technologies. In virtual organizations, partners with separate core competencies can band together temporarily to achieve business objectives. With virtual organizations, the collaborations among partners can break out the time and geographic limitations.

The increasing complexity of e-learning, e-research, and e-business leads to collaboration across multiple disciplines and multiple institutions. Virtual organizations with cross-domain single sign-on that focus on facilitating multiple discipline and multiple institution collaborations are becoming increasingly more predominant. In order to support the collaboration across multiple disciplines and multiple institutions, virtual organizations are required to (1) deal with the new user authentication mechanism in which users are authenticated by distributed user identity management systems (identity providers or IdPs) rather than the local user authentication mechanism; (2) deal with the new resource and service (R&S) protection mechanism in which resources and services are protected by distributed resource and service management systems (service providers or SPs) rather than protected by the local resource and service management system; (3) provide the trust-based authorization mechanisms in which temporary trust relationships between identity providers and service providers are managed and authorization processes that define which user can access which resources or services are based on these trust relationships; and (4) provide a single sign-on (SSO) mechanism to enable users from different identity providers access resources and services from different service providers with only one time sign-on. The benefits result from the new functionalities in virtual organizations and will include: saving the administrators' time and reducing the administrators' costs for identity management and R&S management, reducing the users' sign-on time for accessing R&Ss, and improving the effectiveness of users accessing R&Ss.

The requirements of new functionalities in virtual organizations cause the research and development of new VO authentication and authorization mechanisms that are not found in existing virtual organization systems. Our research provides a trust virtual organization, which extends functionalities of existing virtual organizations, to facilitate the management of distributed users, distributed R&Ss, temporary trust relationships, and access controls. A *Trust Virtual Organization (TVO)* is a virtual organization in which users are authenticated by distributed trusted identity providers, R&Ss are protected by distributed service providers, service providers and identity providers can be set to trust mutually in a certain level, authorization processes are based on the trust relationships, and a single sign-on mechanism enables users access resources and services with one time sign-on. This chapter introduces the trust virtual organization, its motivation, functional model, conceptual models, management components, and an implemented prototype.

BACKGROUND

Since computer-supported cooperative work was proposed in network computing a dozen years ago, Web-based collaborations are widely applied in various areas. Virtual organizations such as Sakai (Sakai, 2007), Moodle (Moodle, 2007), LiveNet (Hawryszkiewycz, 1999), eRoom (E-Room, 2007), and Groove (Rensink, 2003) have become the popular tools supporting Web-based collaborations for learning, research, or businesses.

While many virtual organization systems have been implemented, substantially little is known about the development of virtual organizations with single sign-on and trust-based authorization. In authentication (including single sign-on) aspect, a research project Shibboleth provided by Internet2 (Erdos & Cantor, 2002), however, addressed the design and implementation of a Web-based authentication (including single sign-on) and authorization system. With the Shibboleth, identities of users are managed in distributed identity providers; R&Ss are protected in distributed service providers. That which user can access which R&S is determined by the trust relationships between the identity providers and service providers. Shibboleth project is developed based on the Security Assertion Markup Language (SAML, 2007) as-