Chapter 2.12
Web Services Enabled E-Market Access Control Model

Harry J. Wang
University of Arizona, USA

Hsing K. Cheng
University of Florida, USA

J. Leon Zhao
University of Arizona, USA

ABSTRACT

With the dramtic expansion of global e-markets, companies collaborate more and more in order to streamline their supply chains. Companies often form coalitions to reach the critical mass required to bid on a large volume or wide ranges of products. Meanwhile, they also compete with one another for market shares. Because of the complex relationships among companies, controlling the access to shared information found in e-markets is a challenging task. Currently, there is a lack of comprehensive approach in access control that can be used to maintain data security in e-markets. We propose to integrate several known access control mechanisms such as role-based access control, coalition-based access control, and relationship driven access control into an e-market access control (EMAC) model. In this chapter, we present a web services based architecture for EMAC and the associated concepts and algorithms. We also illustrate via an automotive e-market example how the EMAC model can support e-market access control.

INTRODUCTION

Aimed to make business contact and transactions easier and more cost effective, e-markets have emerged in several industries. For instance, Covisint, an e-market owned by a group of the largest auto manufacturers, is anticipated to handle US $240 billion per year, which is greater than the GDP of Sweden (Feldman, 2000). Many companies have begun the evolution from traditional business practices to e-business to strengthen

customer service, streamline supply chains, and reach existing and new partners.

E-markets open up new possibilities of trade by providing various tools and services. E-catalogs and sourcing directories help both suppliers and buyers increase market visibility, shorten processing time and easily locate business partners (Baron, Shaw, and Bailey, 2000). E-auctions make prices more dynamic and responsive to economic conditions (Feldman, 2000). Scrutiny of the participating companies by e-markets increases the trust between trading partners and makes the establishment of new business relationships easier. Process collaboration tools help companies integrate their processes, which simplifies the work and avoids duplications (eMarket Service, 2002).

As e-markets develop and offer more advanced services, many serious challenges have been presented. Among those challenges, security has been highlighted as a critical issue that must be dealt with for e-markets' attractiveness and profitability. Businesses generally perform controls over the internal use of their business processes. In the e-market environment, this controlled access must be extended to outside the company boundaries (Medjahed, Benatallah, Bouguettaya and Elmagarmid, 2003). Depending on the business situation, participating companies may want e-markets to hide their identities, current trading positions, sensitive catalog items, history or ongoing activity with other players (Feldman, 2000). This gives rise to the need for advanced access control mechanisms.

Although there have been many research efforts in access control in the recent years (Joshi, Aref, Ghafoor and Spafford, 2001), there is a lack of comprehensive methods that can be used directly in the context of e-market access control. We propose to integrate several existing access control models to meet the needs of data security in the presence of complex relationships among companies that participate in an e-market, which we refer to as the *e-market access control* (EMAC) *model*. Among the known access control models, we mainly draw ideas from the models of role-based access control (Sandhu, Coyne, Feinstein and Youman, 1996), task-based access control (Thomas and Sandhu, 1997), coalition-based access control (Cohen, Thomas, Winsborough and Shands, 2002) and relationship-driven access control (Zhao, Wang, Huang and Chen, 2002). We argue that the complex relationships among companies that participate in an e-market require the enforcement of security authorization constraints that are more complex than those found in each of the access control models aforementioned. Therefore, these focused access control models must be integrated into a new access control model that is comprehensive enough to satisfy the needs of e-markets.

In e-markets, the need to interoperate multiple types of systems has risen due to the increased level of connectivity and increased complexity of the data types (Medjahed, Benatallah, Bouguettaya and Elmagarmid 2003). In this chapter, we use web services to enable a distributed architecture for the implementation of the EMAC model, as web services have been embraced by the software industry as the universal standard for open interoperability (Kreger, 2003). We encapsulate advanced security mechanisms inside web services and provide standard interfaces for different security systems to communicate with one another. In particular, we extend some emerging standards such as Security Assertion Markup Language (SAML) and XML Access Control Markup Language (XACML) based on the EMAC model.

Next, we review the relevant literature on access control models. Then, we develop the EMAC model and the related concepts including the four types of relationships, the specification language and the EMAC authorization algorithm. We also present the EMAC architecture that consists of three layers–the inter-organizational workflow layer, the advanced security management layer, and the e-market resources layer. Finally, we