IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITJ2527

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 paper, 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.

Keywords: access control; data security; e-market; inter-organizational workflow; web services

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 paper, 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 summarize our contributions and discuss future research directions.

LITERATURE REVIEW

Ferraiolo et al. (2001) proposed the role-based access control (RBAC) model to simplify management of authorization while providing an opportunity for greater flexibility in specifying and enforcing enterprise-specific protection policies. In the RBAC model, roles represent business functions in a given organization, such as CEO, purchasing manager and buyer. Authorizations are then granted to roles, rather than to single users. The authorizations granted to a role are strictly related to the data objects and resources that are needed for executing the functions associated with the role (Bertino, Bonatti and Ferrari, 2001). Even though RBAC has reached a good maturity level, there are still significant application requirements not addressed by the various versions of RBAC. Therefore, many extensions to RBAC models have been proposed, such as task-based access control (TBAC) and coalition-based access control (CBAC).

Task-based access control uses tasks as an important parameter for access control and authorization (Thomas, 1997; Thomas and Sandhu, 1997). It is an active security model that is well suited for information processing activities, where users access data and applications in order to perform certain tasks. TBAC approaches security management from the application perspective rather than from a system-centric subject-object view. In the subject-object paradigm, the access decision function checks whether a subject has the required permissions for the operation, but it does not take into account the context of the access. In addition, the TBAC paradigm also considers the temporal constraints where access is permitted based on a just-in-time fashion for the activities or tasks in consideration.

Cohen et al. (2002) argued that businesses, governments and other organizations form coalitions to enhance their success. Commercial coalitions include supply chain arrangements, subcontracting relationships and joint marketing campaigns. Such coalitions may be dynamic, as changing conditions and trust relationships result in new missions and modifications to coalition membership. To effectively participate in modern coalitions, member organizations must be able to share specific data and functionality with coalition partners, while ensuring that their resources are safe from inappropriate access. The authors described a family of coalition-based access control (CBAC) models by defining the protection state of a system and the semantics of CBAC-based access policies.

Kang, Park and Froscher (2001) suggested that as more businesses engage in globalization and as inter-organizational collaborative computing grows in importance, the access control requirements for inter-organizational workflow must be met by new access control solutions in a multi-organizational environment. Their proposal emphasized the separation of inter-organizational workflow security from concrete organization level security enforcement.

Further, they described workflow-based access control requirements such as dynamic constraints, fine-grained and context-based access control, and the need to insulate inter-organizational workflows from organization level changes. The role domain was introduced as an interface between workflows and organization-specific security infrastructure.

In B2B e-commerce environments, particularly e-markets, companies form alliances to improve operational efficiency and gain competitive advantages, and meanwhile these companies compete with one another for market shares. The dynamic and complex relationships among companies impose more access control requirements for the shared resources in e-markets, as addressed by the relationship-driven access control (RDAC) model (Zhao, Wang, Huang and Chen, 2002). RDAC states that the access decision of certain shared resources is based on the relationship between access requester company and the owner company of the shared resources. For instance, company X can set an access control policy on its shared e-catalog that any company can see the quantity of the product but only buyer companies can see the price. Here, "buyer companies" is no longer a static role as defined in the role-based access control model. Instead, it represents the dynamic and bidirectional relationship between companies. Therefore, a role-based access control model is not sufficient for access control of shared e-market data. For the same reason, the extended RBAC models like TBAC and CBAC are not sufficient either.

The complexity of various trading functions and dynamic company relationships require e-markets to enforce security authorization constraints that are more complex than those found in each of the access control models aforementioned. Therefore, we propose an EMAC model by integrating all these specialized access control models to satisfy the needs of e-markets. In this paper, we provide guidelines for designing an access control infrastructure in e-markets, and propose a web services enabled architecture and the associated techniques based on emerging web services security standards. To the best of our knowledge, the EMAC model is the first comprehensive access control model specially designed for e-markets.

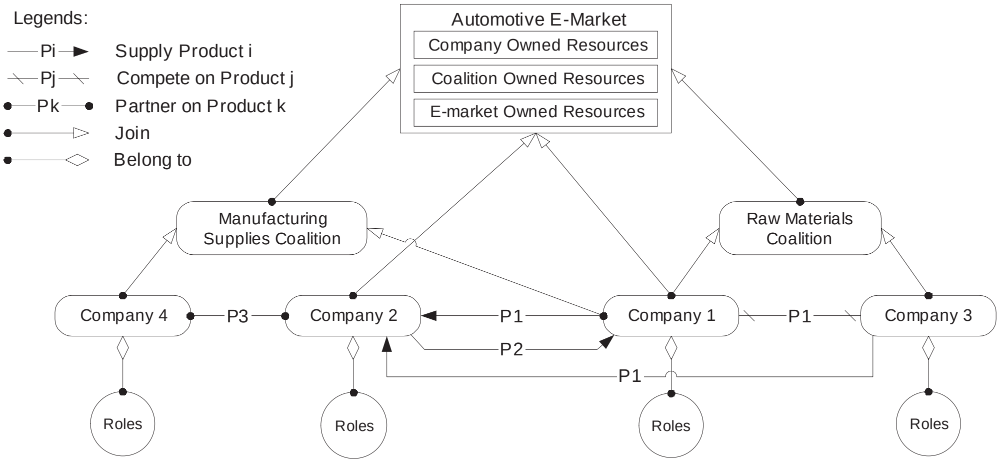
E-MARKET ACCESS CONTROL MODEL

Relationship Hierarchy in E-Markets

Company relationships are important for managing security in an e-market because a company determines information sharing policies based on its relationships with other companies. Figure 1 shows a relationship hierarchy in an automotive e-market, containing four types of relationships.

The first type of relationship is between roles and their companies. Roles have been used as the basic way of authorizing users to access certain information. In the literature, a role is a semantic abstraction of specific job competency within a company (Sandhu, Coyne, Feinstein and Youman, 1996). Role hierarchy is often used to refer to a set of roles found in a company. This relationship is straightforward within a single organizational security domain, while in e-markets this relationship is more complex. In e-markets, users from one security domain need to frequently access protected resources of another security

Figure 1: Relationship Hierarchy in an Automotive E-Market



domain; in this case, roles in one security domain have to be correctly recognized and mapped to another security domain.

The second type of relationship is between two companies. As shown, complex relationships among companies exist. For example, Company 1 is a supplier of Company 2, because Company 1 sells product P1 to Company 2. At the same time, Company 1 is also a buyer of product P2 from Company 2. Company 1 and Company 3 are identified as competitors on P1, because both of them sell the same product P1 to a third party, which is Company 2 in this case. In sum, companies can have multiple relationships between one another.

The third type of relationship is based on the membership of the company in coalitions. In e-markets, small companies often form strategic coalitions to reach the critical mass required to bid on a large volume or wide ranges of products. These coalitions are frequently formed and dissolved as company objectives change. Companies can choose not to join coalitions or to join any number of coalitions. For example, Company 1 participates in both Manufacturing Supplies Coalition and Raw Materials Coalition, while Company 2 is not a member of any coalitions as shown in Figure 1.

The fourth type of relationship is based on the membership of the company in e-markets. E-markets are often closed to companies that are not members. Sometimes only registration is required to become a member, while in other cases companies have to be invited by an existing member or go through a qualification process to get into e-markets (eMarket Service, 2002). Each coalition member company has to register independently to join the e-market regardless if the coalition is a member of the e-market.

Figure 1 also illustrates that shared resources in an e-market are classified into three categories: market-owned resources, coalition-owned resources, and company-owned resources. Market-owned resources include all the trading services and facilities, which are open to all market participating companies subject to certain regulations. Coalition-owned resources are shared among coalition member companies, but its access is also subject to certain access control rules. For instance, a coalition could have various classes of membership with varying privileges. Company-owned resources can be accessed by its employees and by the users of other companies according to certain authorization constraints. Coalition-owned resources and company-owned resources can be stored either by e-markets or by coalition and companies or both. Take e-catalog as an example.Companies can upload their e-catalogs to e-markets or they can host their e-catalogs and only provide links for e-markets to redirect e-catalog access requests.

The Specification of EMAC Model

Figure 2 shows a reference model for the e-market access control (EMAC) that integrates the concepts from RBAC, TBAC and CBAC. We mainly extend the Role-Based Constraints Language 2000 (Ahn and Sandhu, 2000) by incorporating more access control aspects from other models resulting in the E-market Access Control Language (EACL). This language is formal and rigorous since any expression written in EACL can be translated to an equivalent expression in a restricted form of the first-order predicate logic, which can be theoretically studied and reasoned (Bertino, Catania, Ferrari and Perlasca, 2003; Ahn and Sandhu, 2000).

The basic elements and functions on which EACL is based are defined in Figure 3. For specifications related to RBAC, we refer readers to Ahn and Sandhu (2000) and focus the discussion on our extensions in the next subsection. EACL has three new entity sets called tasks (T), companies (C) and coalitions (CO), which are key elements in e-market access control scenarios.

Authorization Constraints

Given the complex relationships in e-markets and various ways of sharing resources, advanced authorization

Figure 2. E-Market Access Control Reference Model

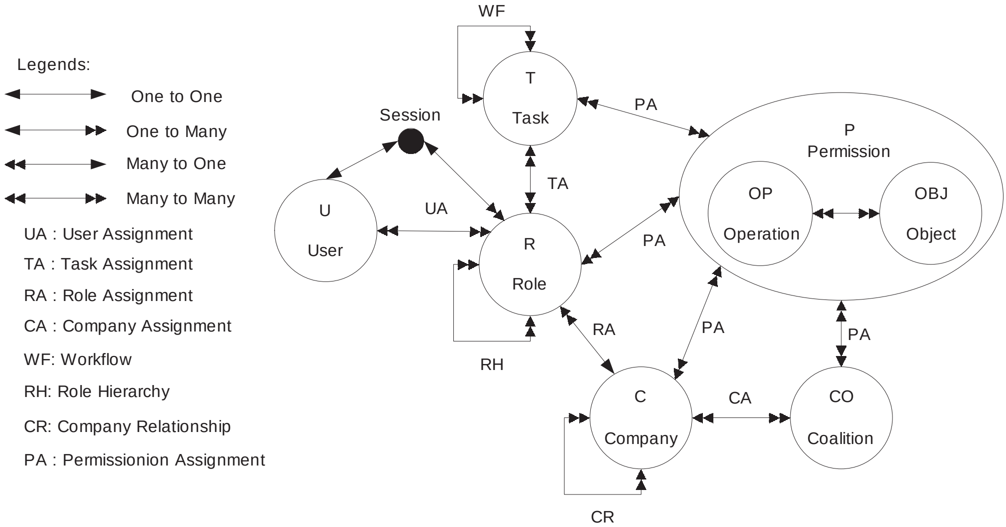


Figure 3. Basic Elements and Functions for E-market Access Control Language (EACL)

U = a set of users, $\{u_1,\ldots, u_i\}$.

R = a set of roles, $\{r_1,\ldots,r_j\}$.

T = a set of tasks, $\{t_1,\ldots t_k\}$.

C = a set of companies, $\{c_1,\ldots,c_l\}$.

CO = a set of coalitions, $\{co_{1,}\ldots,co_m\}$.

OP = a set of operations, $\{op_1,\ldots,op_n\}$.

OBJ = a set of objects, $\{obj_1,\ldots,obj_p\}$.

P = OP × OBJ, a set of permissions, $\{p_1,\ldots,p_q\}$.

S = a set of sessions, $\{s_1,\ldots, s_o\}$.

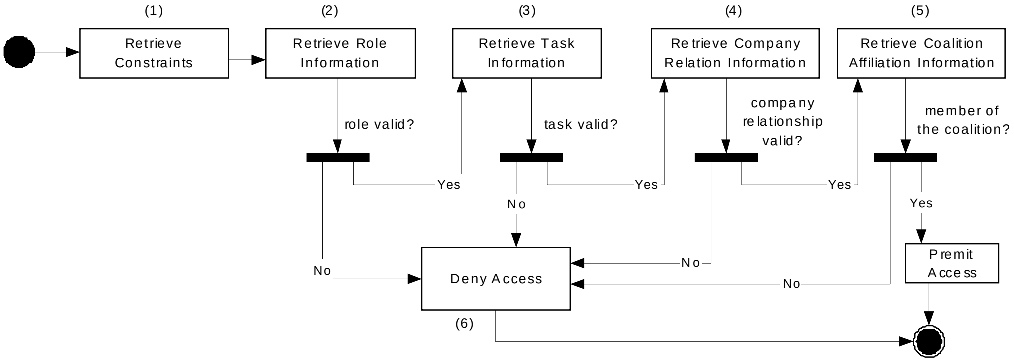
CT = types of classification, {“role”, “task”, “company”, “relationship”, “coalition”}.

RH $\subseteq$ R × R, role hierarchy.
CR $\subseteq$ C × C, company relationships.
WF $\subseteq 2^T$, workflows constituted by a set of tasks.
CLS $\subseteq$ R &T & C&CR&CO, classification of an object.
UA $\subseteq$ U × R, a many-to-many user-to-role assignment relation.
TA $\subseteq$ R × T, a many-to-many role-to-task assignment relation.
RA $\subseteq$ R × C, a many-to-one role-to-company assignment relation.
CA $\subseteq$ C × CO, a many-to-many company-to-coalition assignment relation.
PA $\subseteq$ P × R & P × T & P × C &P × CO, a many-to-many permission assignment relation, which can be permission-to-role, permission-to-task, permission-to-company or permission-to-coalition.
user: $S \rightarrow U$, a function mapping each session s_o to a single user.
user: $R \rightarrow 2^U$, a function mapping each role r_j to a set of users.
role: $U\&P\&S \rightarrow 2^R$, a function mapping the set U, P and S to a set of roles.
task: $T \rightarrow 2^R$, a function mapping each task t_k to a set of roles.
company: $U \rightarrow 2^C$, a function mapping each user u_i to a set of companies.
session: $U \rightarrow 2^S$, a function mapping each user u_i to a set of sessions.
permission: $R\&T\&C\&CO \rightarrow 2^P$, a function mapping the set R, T, C and CO to a set of permissions.
operation: $R \times OBJ \rightarrow 2^{OP}$, a function mapping each role r_j and object obj_p to a set of operations.
relationship: $C \times C \rightarrow 2^{CR}$, a function mapping two companies c_l, c_l’ to a set of company relationships.
affiliation: $C \rightarrow 2^{CO}$, a function mapping company c_l to a set of coalitions.
owner: $OBJ \rightarrow 2^C\&2^{CO}$, a function returns the owner(s) of a object obj_p.
classification: $OBJ \times CT’ \rightarrow 2^{CLS}$, a function mapping each object obj_p and classification type to a set of classifications.

constraints that are more sophisticated than those in existing access control models must be enforced. Being an important aspect of access control, authorization constraints have been extensively studied. As one of the basic security constraints, separation of duty (SOD) is known and practiced long before the existence of computers. The goal of SOD is to reduce the possibility for fraud or significant errors by partitioning the tasks and associated privileges so that cooperation of multiple users is required to complete sensitive tasks (Ahn and Sandhu, 2000). Ferralolo et al. (2001) defined static separation of duty (SSOD) and dynamic separation of duty (DSOD) in the context of role-based access control model. Bertino, Ferrari and Atluri (1999) investigated the enforcement of SOD in workflow management systems. In particular, they systematically addressed the problem of assigning roles and users to tasks in a workflow. Because role-based access control and task-based access control are main components of the EMAC model, all these authorization constraints still hold. In this section, we specify four more authorization constraints from the perspective of shared resources and provide corresponding EACL expressions.

- Role authorization constraints. Conventionally, a role authorization constraint specifies that a user must play certain roles in order to access specific resources and related applications. For instance, company X may only allow other companies' buyers to access its shared e-catalog to improve the confidentiality. The EACL expression for role authorization is | role(U) ∩ classification (OBJ, "role") | >= 1.
- Task authorization constraints. Task authorization constraints have been discussed in the literature such as task-based authorization (Thomas and Sandhu 1997), separation of duties, binding of duties, restricted task execution, and cooperation and inhibition (Casati, Castano and Fugini 2001). Essentially, this constraint specifies that a user must be a participant of certain task to get the access. For example, sometimes the price and quantities of specific products are only visible during the auction (task); when the auction (task) finishes, the access of these information will be revoked. The EACL expression is | task(U)∩ classification (OBJ, "task") | = 1.
- Company authorization constraints. A company authorization constraint expresses an authorization that depends on company relationships. Authorization to company-owned information can be specified based on the user company's relationship with the information owner (Zhao, Wang, Huang and Chen, 2002). In order to reduce computational overhead, authorization can be specified on a higher level of data granularity such as product category instead of product type. This constraint is specified by EACL as: {| C(U) ∩ classification (OBJ, "company") | = 1} ∩ {| relationship(company(U), owner(OBJ)) ∩ classification (OBJ, "relationship") | >= 1}.
- Coalition authorization constraints. A coalition authorization constraint indicates additional privileges for coalition members. An example of coalition authorization is that specific discount information is only accessible to certain classes of member companies of the coalition. In EACL, this is expressed as | affiliation(company(U)) ∩

Figure 4: Authorization Process in EMAC



classification (OBJ, "coalition") | >= 1.

By applying combinations of these four types of authorization constraints, we can support more advanced levels of access control in e-markets. The question is, what happens when those constraints conflict with one another? In this case, we use a "Deny-overrides" (OASIS, 2003) rule to resolve the conflicts. If any one of the four constraints is not satisfied, then, regardless of the evaluation results of the other constraints, the access request is denied. When an access request is received, the EMAC model uses the authorization process shown in Figure 4 to evaluate the access control policies and make the final authorization decision.

This authorization process is sequential while the exact sequence of Step 2 to Step 5 depends on the authorization decision maker's policy. The pseudo code of the EMAC authorization process is given next.

```
INPUT: user $u_i$ and object $obj_p$
OUTPUT: permission $P$
Begin

   If classification($obj_p$, "role") <> N/A Then
    If classification($obj_p$, "role") <> role ($u_i$) Then return FALSE and Exit
    Endif
   Endif

   If classification($obj_p$, "task") <> N/A Then
    If classification($obj_p$, "task") <> task($u_i$) Then return FALSE and Exit
    Endif
   Endif

   If classification($obj_p$, "company") <> N/A Then
    If classification($obj_p$, "company") <> company($u_i$) Then return FALSE and Exit
    Endif
   Endif

   If classification($obj_p$, "relationship") <> N/A Then
    If classification($obj_p$, "relationship") <> relationship(company(($u_i$), owner(OBJ))
      Then return FALSE and Exit
    Endif
   Endif

   If classification($obj_p$, "coalition") <> N/A Then
    If classification($obj_p$, "coalition") <> affiliation(company($u_i$)) Then return FALSE and Exit
    Endif
   Endif

   Return $P$
End
```

An Illustrative Example

Next, we use an example to illustrate how the EMAC model works. Figure 5 describes an e-market trading process.

Figure 6 shows a database schema needed to implement the EMAC access control mechanism. The underlined attributes denote primary keys while foreign keys are in italics.

We can use the following query to get an object's classification constraints information (for ease of presentation, we select names instead of IDs):

```
SELECT o.O_Name, r.R_name,
    T.T_name, C.C_Name, con.C_Type,
    coal.Coal_Name, coal.Permission
FROM Object o, Role r, Task t, Company
    c, Coalition coal, ObjectConstraints
    oc, Constraints con
WHERE con.R_ID = R.R_ID and
    con.T_ID = T.T_ID and con.C_ID =
    C.C_ID and con.Coal_ID =
    coal.Coal_ID and oc.O_ID =
    o.O_ID and oc.ConID =
    con.Con_ID
```

We use the companies in Figure 1 in this example. Suppose at the beginning of the trading process, there is no relationship between Company 1 and 2, and all other relationships are as shown in Figure 1. Raw material manufacturer Company 1 wants to sell aluminum (P1), and in order to improve its business visibility and reach more buyers, it joins the automotive e-market. Table 1 shows the structure of Company 1's e-catalog with the information on aluminum.

Before sharing their e-catalogs, the e-market requires participating companies to classify all the attributes in the e-catalog according to EMAC authorization constraints. Table 2 shows the access control policies for each attribute of the e-catalog in Table 1 defined by Company 1. For instance, the policy of the price is

Figure 5: An E-Market Trading Process

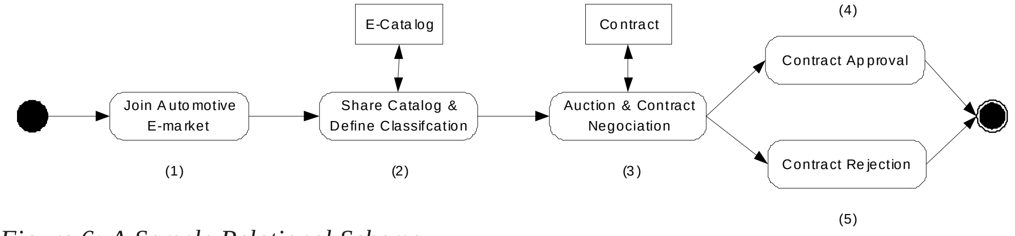


Figure 6: A Sample Relational Schema

User(U_ID, U_Name, Position, Login, Password, *C_ID*)
Role(R_ID, R_Name,R_Desc)
Task(T_ID,T_Name, T_Desc, Start, Expiration, End, *W_ID*)
Workflow(W_ID, W_Name, W_Desc, Start, End)
Company(C_ID, C_Name, Location, Phone, *Coal_ID*)
Coalition(Coal_ID, Coal_Name, Coal_Desc)
Object(O_ID, O_Name, O_Desc, *Con_ID*)
ObjectConstraints (O_ID, Con_ID, Desc)
Constraints(Con_ID, *R_ID*, *T_ID*, *C_ID*, C_Type, *Coal_ID*, Permission, Start, End)
UserRole(U_ID, R_ID, Desc, Status)
UserTask(U_ID, T_ID, Start, End)

defined as follows: the price is only visible to the buyers (role) of companies that have a buying relationship with Company 1 during the auction (task). Except for attributes "Description", "Currency" and "Status", all other attributes have the company relationship constraint as "non-competitor". As a result, an employee from Company 3 can only see the information shown in Table 3 because of the competing relationship between Company 3 and Company 1, which amounts to essentially little information.

Non-buyer employees from all e-market participating companies that are not Company 1's competitors can get more information as shown in Table 4. Price and discount are still not available because of the role constraint on these two attributes.

Now, a buyer from Company 2 named John and another buyer from Company 4 named Tom are searching in the e-market to buy aluminum (P1). Because Company 4 is a member of a manufacturing supplies coalition, Tom can see the discount information besides the information in Table 4. After some initial contacts, both Company 2 and 4 are invited to attend the e-auction held by Company 1. Both John and Tom are involved in the auction (Task 3) and the price of the product is available because the constraints of role, task and relationship are satisfied. When the auction is over, the price is no longer accessible. After the contract negotiation, Company 2 is selected to be the buyer of Company 1 on product aluminum (P1). In order to keep the buying company updated with product

Table 1: An E-catalog Item

Description	Manufacturer	Quant.(ton)	Price/ton	Discount/ton	Currency	Quality	Status
Aluminum	Company 1	2000	500	50	USD	High	Available

Table 2: Access Control Policies Defined by Company 1.

Attribute	Permissio	Role	Task	Company	Relationship	Coalition
Description	Read	N/A	N/A	N/A	N/A	N/A
Manufacter	Read	N/A	N/A	N/A	Non-competitor	N/A
Quant.	Read	N/A	N/A	N/A	Non-competitor	N/A
Price	Read	Buyer	Auction	N/A	Non-competitor	N/A
Discount	Read	Buyer	N/A	N/A	Non-competitor	Manufacturing Supplies Coalition
Currency	Read	N/A	N/A	N/A	N/A	N/A
Qlty.	Read	N/A	N/A	N/A	Non-competitor	N/A
Status	Read	N/A	N/A	N/A	N/A	N/A

Table 3. A Data View to the Employee of Company 3

Description	Manufacturer	Quant.(ton)	Price/ton	Discount/ton	Currency	Quality	Status
Aluminum	###	###	###	###	USD	###	Available

price, Company 1 revises the access control policy of price attribute after establishing the relationship with Company 2. The new policy is presented in Table 5. Now all the buyers from Company 2 can see the price.

This example illustrates the power of the EMAC model. First, role authorization constraints can be easily implemented. Second, when the user moves from one task to another, task authorization constraints take effect. Third, when the company relationship changes by creating a new contract, relationship authorization constraints are activated. Fourth, when a company joins a new coalition, the coalition authorization constraints are triggered. As such, we showed that the EMAC model can accommodate various conventional access control models in a unified manner.

WEB SERVICES ENABLED EMAC ARCHITECTURE

Figure 7 shows a generic access control system architecture (OASIS, 2003) consisting of four system entities for policy administration, storage, enforcement and decision, respectively. Policy Administration Point (PAP) manages all the access control policies and Policy Information Point (PIP) maintains security-related information for subjects, resources and environment. An access requester sends a request for access to the Policy Enforcement Point (PEP), and PEP creates an access decision request to Policy Decision Point (PDP). By evaluating access control policies with attributes of subjects, resources and environment, PDP renders authorization decisions. Finally, PEP executes access control: permit or deny. Each subject is a security autonomy and its intra-organizational access control architecture is similar. But when these autonomies join e-market to collaborate with one another in an e-market, the architecture becomes more complex and more requirements are added.

First of all, cross-company process automation is a fundamental function provided by e-market. Within an individual company, a workflow management system (WFMS) is usually implemented to streamline the business processes. It defines, creates and manages the execution of workflows, interacts with workflow participants and, where required, invokes the use of IT tools and applications. According to the EMAC model, role- and task-related information is required to enforce related constraints and can be acquired from the WFMS. But in an e-market, different companies may have different WFMSs and how to achieve the interoperability among different WFMSs becomes a critical and challenging issue. Second, companies have different access control policies and security systems. In e-markets, these access control policies

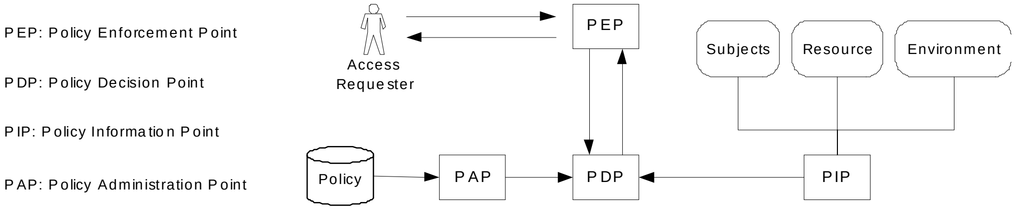
Table 4: A Data View of Non-buyer Employees from Non-competitor Companies

Description	Manufacturer	Quant.(ton)	Price/ton	Discount/ton	Currency	Quality	Status
Aluminum	Company 1	2000	###	###	USD	High	Available

Table 5: Sample New Policy

Attribute	Permission	Role	Task	Company	Relationship	Coalition
Price	Read	Buyer	N/A	N/A	Buying	N/A

Figure 7: A Generic Access Control System Architecture.


PEP: Policy Enforcement Point
PDP: Policy Decision Point
PIP: Policy Information Point
PAP: Policy Administration Point
Access Requester
PEP
Subjects
Resource
Environment
Policy
PAP
PDP
PIP

need to be exchanged and understood by trading partners' security systems. Therefore, how to make disparate security systems communicate with one another imposes another challenge for the e-market access control architecture.

For example, as we have shown, relationships between companies are important for data security in e-markets. But how the relationship information is maintained and where it should be stored are interesting questions. In general, it is not appropriate for the e-market to serve as a centralized relationship information repository, although this method is easy to manage and implement. Because business relationship information is crucial and often top secret for companies, companies are reluctant to let third parties, like e-markets, manage this information. The new e-market access control architecture must support security information exchanges between heterogeneous security systems in order to be successful.

Built on existing and emerging standards such as HTTP, Extensible Markup Language (XML), Simple Object Access Protocol (SOAP), Web Services Description Language (WSDL) and Universal Description, Discovery and Integration (UDDI), web services allow business functions to be loosely integrated between companies more rapidly, easily and less expensively than ever before. They also provide a unifying programming model so that application integration inside and outside the company can be done with a common approach, leveraging a common infrastructure. The integration and application of web services can be done in an incremental manner by using existing languages and platforms and by adopting existing legacy applications (Kreger 2001). These characteristics make web services the ideal enabling technology for our e-market access control architecture.

As shown in Figure 8, we propose a three-layer architecture for the implementation of the EMAC model. Note that our main focus in this paper is on layer 2, and therefore, we will present detailed analysis mainly on this layer.

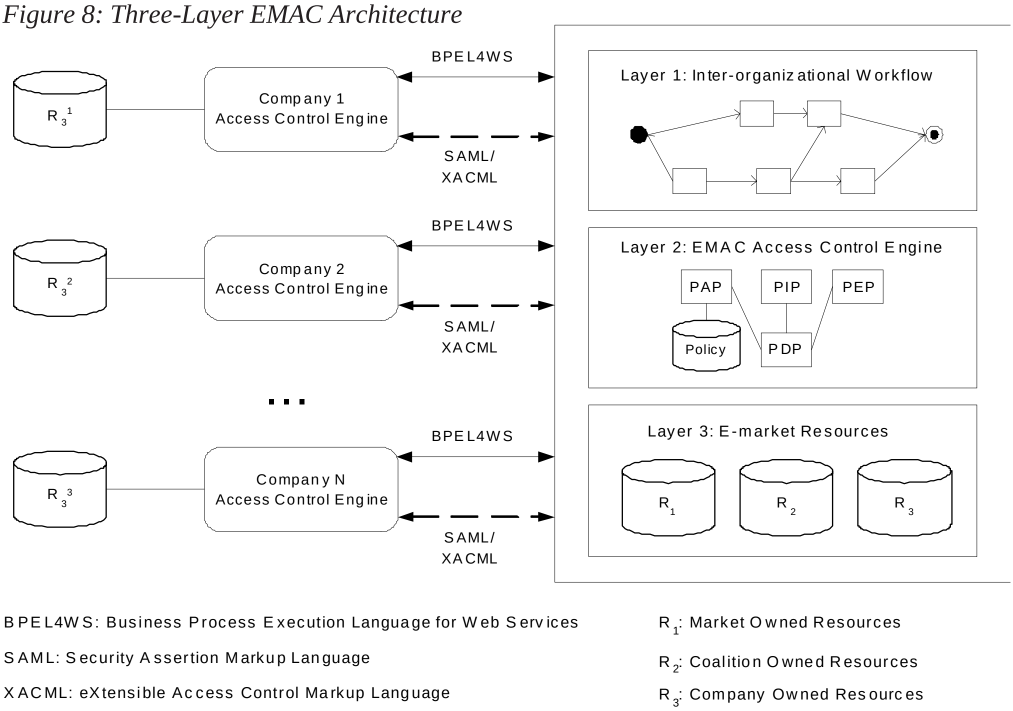
Layer 1 is an inter-organizational workflow composed of tasks wrapped as web services that interface with the private workflows for the companies involved. Based on van der Aalst's definition on various forms of interoperability of inter-organizational workflow, this layer is typically loosely coupled (van der Aalst, 1999). In this layer, business processes are exchanged among business partners with different process execution environments as described in Lee, Yang and Chung (2002) and Leymann, Roller, and Schmidt (2002). The Business Process Execution Language for Web Services (BPEL4WS) –jointly proposed by BEA, IBM and Microsoft–can be used as the inter-organizational workflow definition language (BEA, IBM and Microsoft, 2002). In this way, each e-market participant can define its own business process using whatever process language for internal representation, but we assume that BPEL4WS is used by the e-market for purposes of coordination and synchronization.

The second layer of the architecture is the EMAC access control engine implemented as a web service. This engine communicates with the company security systems, which are also wrapped as web services. This layer is responsible for coordinating with the inter-organizational workflow in Layer 1 to retrieve role and task-related information and issue authorization request and decisions.

In order to support communication between different security systems, Security Assertion Makeup Language (SAML) was proposed (OASIS, 2002). SAML is a technology resulting from the increased trend toward sharing information among different organizations. Although the base technologies behind web services facilitate inter-organizational computing, there had been no standard way of sharing information pertaining to the security domain of an organization with its partner businesses, customers and the like. The cross-domain sharing of security information is addressed by SAML (Nagappan, Skoczylas and Sriganesh, 2003). The security information exchanged is in the form of an assertion about subjects.

There are three types of core assertions defined by the SAML specification: authentication assertion, attribute assertion and authorization assertion. For example, in the example we discussed above, when John from Company 2 wants to see the price of Company 1's aluminum, based on the constraints on price attribute, Company 1's PDP needs an assertion from Company 2 to show whether John's role is buyer. This attribute assertion request and corresponding response are expressed in

Figure 8: Three-Layer EMAC Architecture


R$_3^1$
Company 1 Access Control Engine
BPEL4WS
SAML/ XACML
R$_3^2$
Company 2 Access Control Engine
BPEL4WS
SAML/ XACML
...
R$_3^3$
Company N Access Control Engine
BPEL4WS
SAML/ XACML
Layer 1: Inter-organizational Workflow
Layer 2: EMAC Access Control Engine
PAP
PIP
PEP
Policy
PDP
Layer 3: E-market Resources
R$_1$
R$_2$
R$_3$
BPEL4WS: Business Process Execution Language for Web Services
SAML: Security Assertion Markup Language
XACML: eXtensible Access Control Markup Language
R$_1$: Market Owned Resources
R$_2$: Coalition Owned Resources
R$_3$: Company Owned Resources

SAML as in Listing 1.

In the same manner, Company1's PDP sends another task assertion request to the e-market asking for task information in which John is currently involved. Based on the business process defined in BPEL4WS, the e-market returns a task name. Finally, after checking the relationship between Company 2 and Company 1, the PDP issues an authorization decision to PEP. Applications working with SAML can define their own specific assertions. However, this extensibility comes at the cost of interoperability. In this situation, e-markets can provide a standard specification of SAML assertions that all participants must follow.

As we can see in this example, the security policies or access control authorization constraints of each e-market participant have many elements and many points of enforcement. They may be enforced by different departments within the company or by external business partners or e-markets. For this reason, there is a pressing need for a common language to express security policy. The eXtensible Access Control Markup Language (XACML) is a technology that enables access control policies to be expressed in a standard XML format (OASIS, 2003). It defines a syntax that SAML can leverage for expressing current values used by the policies. By extending XACML, all the authorization constraints

Listing 1: SAML Assertion Request and Response

```
    Role assertion request from Company 1:
    <samlp:Request>
          <samlp:AttributeQuery>
                 <saml:Subject>
                        <saml:NameIdentifier SecurityDomain =”Company 2"
                         Name=”John”/>
                 </saml:Subject>
                 <saml:AttributeDesignator AttributeName=”role”
                 AttributeNamespace=”Company 2"/>
          </samlp:AttributeQuery>
</samlp:Request>
    Role assertion response from Company 2:
    …
<samlp:Response ...>
   <saml:Assertion ...>
          <saml:Conditions .../>
          <saml:AttributeStatement>
                 <saml:Subject>
                        <saml:NameIdentifier SecurityDomain =”Company 2"
                         Name=”John”/>
                 </saml:Subject>
                 <saml:Attribute AttributeName=”role”
                  AttributeNamespace=”Company 2"/>
                 <saml:AttributeValue>buyer</saml:AttributeValue>
          </saml:AttributeStatement>
   </saml:Assertion ...>
</samlp:Response>
…
```

in EMAC models can be specified in a standard way. For example, the access control policy for attribute price is that the price is only visible to the buyers of companies that have a buying relationship with Company 1 during the auction, which can be expressed in the extended XACML as shown in Listing 2.

Layer 3 consists of the e-market resources, which include three types, namely, market-owned resources, coalition-owned resources, and company-owned resources as explained previously. Market-owned resources are centrally controlled by e-markets, while the management of the other two types of resources is due to their owners: coalitions and companies, respectively. There are various ways of linking the coalition and company owned resources to the e-market. The relevant contents of a company database can be either uploaded physically to the e-market database or linked logically (Geppert, Kradolfer, & Tombros, 1998). As a result, the access control to the company-owned resources may vary depending on whether or not the data are uploaded to the e-market.

These three layers are loosely coupled and can exist independently, which provides the flexibility and scalability that are important for the fast-growing e-markets. The detailed analysis of lower level implementation algorithms are beyond the scope of this paper.

CONCLUSIONS

A variety of access control models have been developed in response to system and security administration requirements. Particularly, role-based access control

Listing 2. An XACML Policy

```
<?xml version=1.0" encoding=”UTF-8"?>
<Policy xmlns=”urn:oasis:names:tc:xacml:1.0:policy”
xmlns:xsi=”http://www.w3.org/2001/XMLSchema-instance”
xsi:schemaLocation=”urn:oasis:names:tc:xacml:1.0:policy
http://www.oasis-open.org/tc/xacml/1.0/cs-xacml-schema-policy-01.xsd”
PolicyId=”identifier:example:Company1SamplePolicy”
RuleCombiningAlgId=”identifier:rule-combining-algorithm:deny-overrides”>
<Description>
    Company 1 Access Control Policy
</Description>
<Target>
    <Subjects>
            <AnySubject/>
    </Subjects>
    <Resources>
            <AnyResource/>
    </Resources>
    <Actions>
            <AnyAction/>
    </Actions>
</Target>
<Rule RuleId= “urn:oasis:names:tc:xacml:1.0:example:SimpleRule1” Effect=”Permit”>
    <Description>
            price is only visible to the buyers of companies that have buying
            relationship with Company 1 during the auction.
    </Description>
```

```
<Target>
    <Subjects>
        <Subject>
            <SubjectMatch MatchId=”
            urn:oasis:names:tc:xacml:1.0:function:Role-match”>
            <SubjectAttributeDesignator
            AttributeId=”urn:oasis:names:tc:xacml:1.0:subject:user-role”
            DataType=”urn:oasis:names:tc:xacml:1.0:data-type:Role”/>
            <AttributeValue
            DataType=”urn:oasis:names:tc:xacml:1.0:
            datatype:Role”>buyer
            </AttributeValue>
            </SubjectMatch>

            <SubjectMatch MatchId=”
            urn:oasis:names:tc:xacml:1.0:function:task-match”>
            <SubjectAttributeDesignator
            AttributeId=”urn:oasis:names:tc:xacml:1.0:subject:user-task”
            DataType=”urn:oasis:names:tc:xacml:1.0:data-type:Task”/>
            <AttributeValue
            DataType=”urn:oasis:names:tc:xacml:1.0:
            datatype:Task”>auction
            </AttributeValue>
            </SubjectMatch>

            <SubjectMatch MatchId=”
            urn:oasis:names:tc:xacml:1.0:function:relationship-match”>
            <SubjectAttributeDesignator
            AttributeId=”urn:oasis:names:tc:xacml:1.0:subject:company-
                         relationship”
            DataType=”urn:oasis:names:tc:xacml:1.0:data-
                        type:Relationship”/>
            <AttributeValue
            DataType=”urn:oasis:names:tc:xacml:1.0:
            datatype:Relationship”>buying
            </AttributeValue>
            </SubjectMatch>
        </Subject>
    </Subjects>
    <Resources>
        <Attribute AttributeId=”urn:oasis:names:tc:xacml:1.0:resource:ufspath”
            DataType=”http://www.w3.org/2001/
                        XMLSchema#anyURI”>
        <AttributeValue>Company1/ProductCatalog/attribtes/price</
                      AttributeValue>
        </Attribute>
    </Resources>
    <Actions>
        <Attribute AttributeId=”urn:oasis:names:tc:xacml:1.0:action:action-id”
            DataType=”http://www.w3.org/2001/XMLSchema#string”>
        <AttributeValue>read</AttributeValue>
        </Attribute>
    </Actions>
</Target>
```

(RBAC) (Sandhu, Coyne, Feinstein and Youman, 1996), task-based access control (TBAC) (Thomas and Sandhu, 1997), and team-based access control (TMAC) (Thomas, 1997) use “role”, “task” and “team” respectively to model contextual information associated with organizational roles, task responsibilities and collaborative activities (Cohen, Thomas, Winsborough and Shands, 2002). The Coalition Based Access Control (CBAC) model discusses, for the first time, the relationship between organizations through the memberships in a coalition. The Relationship Driven Access Control model takes into account the direct relationships between companies and proposes an object classification scheme (Zhao, Wang, Huang and Chen, 2002).

In this paper, we studied the resource sharing problem in the e-market by analyzing the relationships among companies and identifying four types of authorization constraints. By integrating several access control models, we proposed a comprehensive security control mechanism called the E-Market Access Control (EMAC) model to support advanced access control in e-markets. Another thrust of this study is the adoption of web services as the implementation platform, leading to a loosely coupled, three-layer EMAC architecture. The three layers are the inter-organizational workflow, the advanced security control web services and the e-market resources. We have demonstrated the feasibility of this architecture and the comprehensive access control mechanism. Our future research plan includes the detailed analysis and design of algorithms for the EMAC system, the development of an EMAC prototype and its application in a realistic e-market case.

REFERENCES

Ahn, G. & Sandhu, R. (2000). Role-based authorization Constraints Specification. *ACM Transactions on Information and System Security*, 3(4), 207-226.

Baron, J. P., Shaw, M. J., & Bailey, A. D. (2000). Web-based e-catalog systems in B2B procurement. *Communications of the ACM*, 43(5), 93-100.

BEA System, IBM Corporation and Microsoft Corporation, Inc. (2002) Business Process Execution Language for Web Services, Version 1.0. http://www.bim.com/developerworks/library/ws-bpel .

Bertino, E., Bonatti, P. A., & Ferrari, E. (2001) TRBAC: A Temporal Role-Based Access Control Model, *ACM Transactions on Information and System Security*, 4(3), 191-223.

Bertino, E., Catania, B., Ferrari, E. & Perlasca, P. (2003). A logical framework for reasoning about access control models. *ACM Transactions on Inofrmation and System Security*, 6(1), 71-127.

Bertino, E., Ferrari, E. & Atluri, V. (1999). The specifiction and enformcement of authorization constraints in workflow management systems. *ACM Transactions on Information and System Security*, 2(1), 65-104.

Casati, F., Castano, S. & Fugini, M. (2001) Managing Workflow Authorization Constraints through Active Database Technology. *Information Systems Frontiers*, 3(3), 319-338.

Cohen, E., Thomas, R.K., Winsborough, W. & Shands, D. (2002) Models for Coalition-based Access Control (CBAC). *Seventh ACM Symposium on Access Control Models and Technologies*, Monterey, California.

eMarket Services. (2002).

Introduction to eMarkets. http://www.emarketservices.com.

Feldman, S. (2000). Electronic marketplaces. *IEEE Internet computing*, July-August, 93-95.

Ferralolo, D. F., Sandhu, R., Gavrila, S., Kuhn, D. R. & Chandramouli, R. (2001). Proposed NIST Standard for Role-based Access Control. *ACM Transactions on Information and System Security*, 4(3), 224-274

Geppert, A., Kradolfer, M. & Tombros, D. (1998) Federating heterogeneous workflow systems. *Technical Report* 05, Department of Computer Science, University of Zrich.

Joshi, J. B. D., Aref, W. G., Ghafoor, A. & Spafford , E. H. (2001) Security models for web-based applications. *Communications of the ACM*, 44(2), 38-44.

Kang, H.M., Park, J.S. & Froscher, J.N. (2001) Access Control Mechanisms for Inter-organizational Workflow. *6th ACM Symp. on Access Control Models and Technologies*, 66-74.

Kreger, H. (2003) Fulfilling the Web services promise, *Communications of the ACM*, (46)6, 29-34.

Kreger, H. (2001) Web Services Conceptual Architecture. *IBM Software Group*, May 2001. http://www-3.ibm.com/software/solutions/webservices/pdf/WSCA.pdf.

Lee, J., Yang, J. & Chung, J. (2002) Winslow: A Business Process Management System with Web Services. Technical Paper, IBM T.J. Watson Research Center.

Leymann, F., Roller, D. & Schmidt M.T. (2002) Web services and business process management. *IBM Systems Journal, Special Issue on New Developments in Web Services and E-commerce*, 41(2), 198-211.

Medjahed, B., Benatallah, B., Bouguettaya, A., Ngu, A. H. H., & Elmagarmid, A. K. (2003). Business-to-business interactions: issues and enabling technologies. *The VLDB Journal*, 12, 59-85.

Nagappan, R., Skoczylas, R. & Sriganesh, R. P. (2003). *Developing Java Web Services*. John Wiley & Sons.

OASIS (2003). eXtensible access control markup language (XACML) version 1.0. http://www.oasis-open.org/committees/xacml/repository/.

OASIS (2002). Assertions and protocol for the OASIS security assertion markup language (SAML). http://www.oasis-open.org/committees/security/docs/.

Sandhu, R.S., Coyne, E.J., Feinstein, H.L. & Youman, C.E. (1996) Role-based Access Control Models. *IEEE Computer*, 29(2), 38 -47.

Thomas, R. K. (1997) Team-based Access Control (TMAC): A Primitive for Applying Role-based Access Controls in Collaborative Environments. *2nd ACM Workshop on Role-Based Access Control*, Nov. 6-7, 13 -19.

Thomas, R.K. & Sandhu, R.S. (1997) Task-based Authorization Controls (TBAC): A Family of Models for Active and Enterprise-oriented Authorization Management. *Proceedings of the IFIP WG11.3 Workshop on Database Security*, Lake Tahoe, California, August 11-13.

van der Aalst., W.M.P. (1999) Interorganizational Workflows: An Approach based on Message Sequence Charts and Petri Nets. *Systems Analysis - Modelling–Simulation*. 34(3), 335-367.

Zhao, J. L., Wang, H. J., Huang, S. S. & Chen, G. (2002) Relationship driven access control in a supply web. *Proceedings of the 12th Workshop on Information Technology and Systems (WITS'O2)*, Barcelona, Spain.

Harry J. Wang is a third year PhD student of MIS at the University of Arizona. He holds a Bachelor degree in MIS from Tianjin University, the People's Republic of China. His research interests involve access control in e-commerce, workflow technologies and applications, and web services. He has published in the Workshop on Information Technology and Systems, Barcelona, Spain, 2002, and in the First International Conference on Web Services, Las Vegas, 2003.

Hsing "Kenny" Cheng is Associate Professor of Information Technology and the American Economic Institutions Faculty Fellow at the Department of Decision and Information Sciences of Warrington College of Business Administration at the University of Florida. Prior to joining UF, he served on the faculty at The College of William and Mary from 1992 to 1998. He received his Ph.D. in computers and information systems from William E. Simon Graduate School of Business Administration, University of Rochester in 1992. Dr. Cheng's research interests involve electronic commerce, economics of information systems, and information technology in supply chain management. His recent research focuses on modeling the impact of Internet technology on software development and marketing, and issues surrounding the application services supply chain and web services. His work has appeared in Computers and Operations Research, Decision Support Systems, European Journal of Operational Research, IEICE Transactions, Journal of Business Ethics, Journal of Information Systems and e-Business Management, Journal of Management Information Systems, and Socio-Economic Planning Sciences. Dr. Cheng is a member of ACM, DSI, and INFORMS.

J. Leon Zhao is Honeywell Fellow and Associate Professor of MIS, University of Arizona. He holds PhD degree from University of California, Berkeley, MS degree from University of California, Davis, and Bachelor degree from Beijing Institute of Agricultural Mechanization. He has previously taught in Hong Kong University of Science and Technology and College of William and Mary. His research interests include applications integration, e-learning, e-market security, knowledge management, process modeling and verification, workflow management systems, and web services technology. He has published over 70 research articles in academic journals and referred conferences, including such journals as Management Science, Information Systems Research, Communications of the ACM, Journal of Management Information Systems, and IEEE Transactions on Data and Knowledge Engineering. He is associate editor for Electronic Commerce Research and Applications and for International Journal of Web Services Research and serves on the editorial board of Journal of Database Management. He has co-edited two special issues in workflow management and is co-editing a special issue on Web Services and Process Management for Decision Support Systems.