Integrated Resource and Logistics Management through Secure Information Sharing for Effective Emergency Response

Vijayalakshmi Atluri[1], Soon Ae Chun[1], John Ellenberger[2], Basit Shafiq[1], Jaideep Vaidya[1]
{atluri, soon, shafiq, jsvaidya}@cimic.rutgers.edu, john.ellenberger@sap.com
[1]CIMIC, Rutgers University, [2]SAP Research

1. Introduction

A disaster, either natural or man-made, can occur at any time and place. In either case, it leads to an emergency situation which must be promptly and appropriately responded to. In the USA, as in many parts of the world, governmental agencies, non-governmental organizations, and even private sector companies may co-operate and co-ordinate the response. Indeed, while the primary response to an emergency situation is coordinated by the public sector, many of the supplies crucial to recovery such as food, fuel, building supplies flow through private (retail and wholesale) channels. These large commercial suppliers employ sophisticated supply chain and logistics systems, which track the availability and location of their inventory. Unfortunately, this information is only available anecdotally to officials responsible for coordinating the recovery effort which leads to a less effective recovery effort.

The primary reason for this in general is the autonomy and lack of information sharing among the cooperating agencies, institutions, and even individuals. Information sharing is hindered by a number factors including lack of interoperability and standards among the agencies data format, semantics, applications and systems in use, as well as diverse information sharing requirements for protecting the privacy and security needs of the organization, and lack of effective inter-organizational information sharing strategies and practices. In addition to information sharing, resource management coordination for effective emergency management coordination requires process-level interoperability among the various response agencies/organizations.

As the entire resource supply pipeline can be viewed as a global supply chain, it is obvious that the lack of timely and accurate information creates supply inefficiencies and less than optimal resource distribution. This severely hampers any relief efforts. It is critical that this resource information including the respective supply chains as well as the regulations to share the needed resources should be exchanged among the required entities in a seamless fashion for an effective and timely response. Enabling such information sharing is critical for: i) identifying the resource and logistics requirements for emergency response operations such as evacuation, sheltering, food and medical supply, infrastructure restoration; ii) discovering appropriate agencies/organizations that can collectively satisfy the resource requirements; iii) integrating allocation, tasking, dispatch, and mobilization processes along the resource supply chain across various agencies/organizations to ensure timely delivery of needed resources.

To solve this problem, we envision a system that enables secure and fine grained controlled sharing of private supply chain information with emergency response teams for the purpose of helping with needs priorities, distribution, and logistics coordination. We now examine some of the specific research challenges in building such a system.

2. Research Challenges

In general, secure information sharing and interoperability in necessary in two different settings: when the entities involved are known *apriori* and when they are not known in advance but decided in an ad-hoc and dynamic manner. This necessitates approaches that enable agencies to interoperate without compromising their security policies. For an established coalition, it is necessary to compose a global security policy from the local policies of agencies after resolving their policy differences and conflicts. This global policy governs information sharing among agencies based on their roles and responsibilities. For ad-hoc coalitions, approaches must be developed to allow secure information sharing among agencies without having to pre-negotiate their policies, but yet preserve individual agencies' security policies. This involves discovering collaborative security policies from existing access control data, and enforcing them.

In addition to information sharing, resource management coordination for effective emergency management coordination requires process-level interoperability among the various response agencies/organizations. In case of established

coalition, such process-level interoperability can be easily developed as the agencies/organizations and their business processes are known a priori and can be integrated for the various emergency support functions. However, in dynamic ad hoc coalition environment achieving process-level interoperability poses a significant challenge as such coalition is formed for short term basis among organizations without complete knowledge about their business processes. Moreover, due to privacy and business concerns organizations may be reluctant to provide complete details about their processes for resource supply chain. A secure and privacy-preserving process composition approach must be developed to serve such needs. We now look at these issues.

2.1 Policy-Based Secure Information Sharing

Among established coalition members, interoperability and information sharing can be established based on a global interoperation policy. Such an interoperation policy can be composed from the established local policies of the collaborating agencies to ensure that all the security and access control constraints of these agencies are incorporated in the global policy. Composition of such global interoperation policy is a challenging task and requires resolving differences and conflicts among the policies of the collaborating agencies. This requires examining the following key issues:

i) Policy Differences: Policy differences occur due to semantic heterogeneity among the policies of different agencies. Semantic heterogeneity may arise due to naming differences, structural differences and constraint differences. Naming differences occur when agencies use similar names to represent different conceptual entities or different names to represent the same conceptual entities. Structural and constraint differences arise as agencies may represent similar conceptual entities in different structure and may have different constraints among their entities.

ii) Policy Conflicts: Interoperation conflicts may arise due to contradictory authorizations and restrictions in the security and access control policies of collaborating organizations. These authorizations and restrictions may be context sensitive and therefore detection and resolution of such conflicts cannot be achieved by simple syntactic comparison of the policies of collaborating agencies [Lup99,Yan02, Pot03]. With reference to security and access control policies, conflicts can be divided into state-independent conflicts and state-dependent conflicts, which require different solutions. For state-independent conflicts, one solution may be to build on existing work on policy composition [Sha05, Sha06] where policy conflicts are resolved in an iterative manner using the integer programming model. For state-dependent conflicts, it is necessary to represent the context sensitive policies of collaborating agencies in state-space models such as state machines, Petri Nets, Modecharts, or timed automata [Ber91, Ost90, Alu94]. Conflicts amongst such state-based representation of policies can now be detected by employing model checking.

For ad-hoc coalitions one cannot predict and prepare for all eventualities and therefore may not have the prior knowledge of the agencies involved to respond to the emergency at hand. Moreover, coalitions evolve as the situation develops, changes within each member agencies procedures and policies occur. Even if the coalition was formed in a quick manner and dynamic in nature, efficient and secure solutions are needed to form and maintain the electronic collaborations. Agencies should be able to exercise their own local fine-grained access control policies while sharing resources with external entities.

Although this may be accomplished by means of traditional access control and authentication mechanisms, they are administratively difficult when the coalitions and interactions are short-lived and constantly changing. This is because, using traditional access control would require explicit specification of authorizations for individual users within each member organization and changes would need to be painstakingly administered, which is not possible given the scope of organizations and the compressed timelines forced by emergencies.

One possibility is to utilize a coalition based access control model which can automatically translate system level access control policies into implementation level policies that will have varying levels of security and restrictiveness. Thus, if one can identify the credentials that determine the role and therefore allow one to gain access to a resource, then we can test if an external user possesses the same (or similar) credentials to give him access to that object. Our prior work [Atl04, War05, War05a, War07] addresses some of these issues.

Alternatively, it may be possible to mine collaborative security policies by employing data mining techniques to achieve secure dynamic sharing. The goal of this mining is to come up with a common understanding of the security policies across different organizations participating in the collaboration in order to facilitate automatic and secure collaborative resource sharing. Our work on role engineering [Vai06, Vai07, Vai08] addresses this

issue. In particular, we can translate local access control policies into a common Role based access control (RBAC) policy because RBAC is perceived to be policy neutral and because it does not require policies to be set on individual subjects for the collaboration, an invaluable feature for coalitions that frequently change. Once such a common RBAC policy is discovered, then it forms a basis for entertaining external users' access requests for local resources.

2.2 Ontology Driven Collaborative Resource Management

While information sharing enables the free flow of information between response partners, it cannot actively co-ordinate a comprehensive global response. Indeed, the emergency response process can be viewed as a workflow of activities with certain resource requirements. Depending on resource requirements and jurisdictions, the activities in a response process need to be executed by different agencies/organizations in coordination with each other. Given the dynamic nature of the emergency management environment and the differences in the roles, responsibilities of the agencies/organizations and the resources they can provide, appropriate response plans must be formulated that satisfy all of the requirement constraints.

An ontology-based inference framework may assist the process designer and incident commander in planning and execution of the response processes for the emergency. This requires that the emergency management ontology be specified in a formalism that supports automated inferences such as default actions and resources for a given emergency situation, as well as organizations responsible for performing these actions and providing the needed resources. It is not feasible to do such inferencing in advance, since, for example, resource availability with enterprises depends on their supply chain and changes dynamically. Moreover, the rules of agencies may themselves get changed. Therefore, a dynamic and scalable inferencing approach is essential in this environment. For such automated inferences, we can build on our ontology-based reasoning work [Sha08].

2.3 Process-level Interoperability

We now require a seamless way of incorporating orders, demand and supply information in a real-time fashion. For any given organization, there is a business process for resource request, allocation, tasking, dispatch, and delivery. To ensure the timely delivery of resources, the underlying business processes of the response agencies need to be well coordinated to satisfy the requirements and constraints of the overall response process.
This requires verifying that the individual processes can be composed to accomplish all the tasks in the overall response process workflow under the given constraints. These constraints may be related to the ordering and temporal dependency between workflow tasks. In addition, these constraints may be manifested as policy requirements.

Each task in the overall emergency response process may expand to a sub-workflow of the response agency/organization which may again be expanded as sub-workflows at the next level. The control and information flow dependencies are represented as control-flow and information flow graphs. However, the event ordering and policy-level constraints cannot be represented in the control/information flow graph as the underlying events may correspond to the sub-workflow tasks at lower level and these tasks may not be visible to workflow designer at the higher-levels. Clearly, private organizations and suppliers may not provide complete disclosure of their individual business processes, sub-workflows, and local supply-chains.

The constraints on the global workflow pertaining to the occurrence of events in the sub-workflows can be represented as in event-based models including scenario diagrams [Bon05, Bra05] and temporal logic models [Cla86, Sis82, Dav98, Dav04, Rom07] and concurrent transaction logic (CTR) [Rom07]. We can model the process-level interoperability for emergency response composition as a Web service composition problem where the response agencies/organizations provide access to their resources and data as Web services.

To do this, we perform bottom-up and incremental composition of the Web Service Process (WSP) execution plan along the service composition hierarchy. This hierarchy is established based on the roles of response agencies/organizations as service requester or service provider at different levels of the composition. At the lowest level (level = 0), the original WSP is the service requester and the component Web services that have direct interaction with the WSP as service providers. At the next level these service providers become service requesters and the component Web services invoked by them are the service providers and so on.

At each hierarchy level, the execution plan of the cascaded Web services at that level is verified for conformance with the WSP specifications and constraints of service providers/requesters.

References

[Alu94] R. Alur, D.L. Dill, “A Theory of Timed Automata,” Theoretical Computer Science, vol. 126, no. 2, Apr. 1994, pp. 183-236.

[Atl04] V. Atluri and J. Warner, “Automatic Enforcement of Access Control Policies among Dynamic Coalitions,” International Conference on Distributed Computing and Internet Technology, December 2004.

[Ber91] B. Berthomieu and M. Diaz, “Modeling and Verification of Time Dependent Systems using Time Petri Nets,” IEEE Trans. Software Eng., vol. 17, no. 3, Mar. 1991, pp. 259-273.

[Bon05] Y. Bontemps and P. Heymans, “From Live Sequence Charts to State Machines and Back: A Gided Tour,” IEEE Trans. Softw. Eng., 31(12):999–1014, 2005.

[Bra05] V. Braberman, N. Kicilof, and A. Olivero, “A Scenario-Matching Approach to the Description and Model Checking of Real-Time Properties,” IEEE Trans. Software Eng., vol. 31, no. 12, 2005, pp. 1028-1041.

[Cla86] E. M. Clarke, E. A. Emerson, and A. P. Sistla, “Automatic Verification of Finite-state Concurrent Systems using Temporal Logic Specifications,” ACM Trans. Program. Lang. Syst., 8(2):244–263, 1986.

[Dav98] H. Davulcu, M. Kifer, C. R. Ramakrishnan, and I. V. Ramakrishnan, “Logic Based Modeling and Analysis of Workflows,” In PODS ’98: Proceedings of the seventeenth ACM SIGACT-SIGMOD-SIGART symposium on Principles of database systems, 1998.

[Dav04] H. Davulcu, M. Kifer, and I. V. Ramakrishnan, “Ctr-s: A Logic for Specifying Contracts in Semantic Web Services,” In WWW Alt. ’04: Proceedings of the 13th International World Wide Web conference on Alternate track papers & posters, 2004.

[Lup99] E. Lupu and M. Sloman, “Conflicts in Policy-Based Distributed Systems Management,” IEEE Trans. Software Eng., vol 25, no. 6, pp. 852-869, Nov. 1999.

[Ost90] J. Ostroff. Temporal Logic of Real-time Systems. Research Studies Press, 1990.

[Rom07] D. Roman and M. Kifer, “Reasoning about the Behavior of Semantic Web Services with Concurrent Transaction Logic,” In VLDB ’07: Proceedings of the 33rd international conference on Very large data bases, VLDB Endowment, 2007.

[Sha05] B. Shafiq, J. Joshi, E. Bertino, and A. Ghafoor, “Secure Interoperation in a Multi-Domain Environment Employing RBAC Policies” IEEE Trans. Knowledge and Data Eng., vol. 17, no. 11, pp. 1551-1577, Nov. 2005.

[Sha06] B. Shafiq. Access Control Management and Security in Multi-Domain Collaborative Environments. PhD thesis, School of Electrical and Computer Engineering, Purdue University, August 2006. CERIAS TR 2006-19.

[Sha08] B. Shafiq, J. Vaidya, V. Atluri, N.Adam, S. Chun, and A. Lieb, "Ontology Driven Resource Management for Emergency Response," in Proceedings of the Workshop on Secure Knowledge Management (SKM 2008), November 3-4, 2008.

[Sis82] A. P. Sistla and E. M. Clarke, “The Complexity of Propositional Linear Temporal Logics,” In STOC ’82: Proceedings of the fourteenth annual ACM symposium on Theory of computing, 1982.

[Vai06] J. Vaidya, V. Atluri, and J.Warner. Roleminer: mining roles using subset enumeration. In CCS ’06: Proceedings of the 13th ACM conference on Computer and communications security, pages 144–153, 2006.

[Vai07] J. Vaidya, V.Atluri, and Q. Guo. The role mining problem: Finding a minimal descriptive set of roles. In ACM Symposium on Access Control Models and Technologies, pages 175–184, 2007.

[Vai08] J. Vaidya, V.Atluri, Q. Guo, and N. Adam. Migrating to Optimal RBAC with Minimal Perturbation. In ACM Symposium on Access Control Models and Technologies, pages 11–20, 2008.

[War05] J. Warner, V. Atluri, and R. Mukkamala, “An Attribute Graph Based Approach to Map Local Access Control Policies to Credential Based Access Control Policies. In ICISS, pp. 134- 147, 2005.

[War05a] J. Warner, V. Atluri, and R. Mukkamala, “A credential-based approach for facilitating automatic resource sharing among ad-hoc dynamic coalitions,” In IFIP, August 2005.

[War07] J. Warner, V. Atluri, R. Mukkamala and J. Vaidya, “Using Semantics for Automatic Enforcement of Access Control Policies among Dynamic Coalitions,” In ACM Symposium on Access Control Models and Technologies, 2007.

[Yan02] G. Yan, W.K. Ng, and E. Lim, “Product Schema Integration for Electronic Commerce–A Synonym Comparison Approach,” IEEE Trans. Knowledge and Data Eng., vol. 14, no. 3, pp. 583-598, May/June 2002.