Available online at www.sciencedirect.com
ScienceDirect
Electronic Notes in Theoretical Computer Science
ELSEVIER
Electronic Notes in Theoretical Computer Science 179 (2007) 97–109
www.elsevier.com/locate/entcs

Secure Information Sharing in a Virtual Multi-Agency Team Environment [1]

Nabil Adam,[2] Ahmet Kozanoglu,[3]
Aabhas Paliwal[4] and Basit Shafiq[5]

CIMIC, Management Science & Information Systems
Rutgers University
NJ, USA

Abstract

This paper proposes a two tier RBAC approach for secure and selective information sharing among virtual multi-agency response team (VMART) and allows expansion of the VMART by admitting new collaborators (government agencies or NGOs) as need arise. A coordinator Web Service for each member agency is proposed.The coordinator Web Service is responsible for authentication, information dissemination, information acquisition, role creation and enforcement of predefined access control policies. Secure, selective and fine-grained information sharing is realized through the encryption of XML documents according to RBAC policies defined for the corresponding XML schema.

Keywords: XML, RBAC, Virtual Team, Access Control, Information Sharing, SOA, Web Services

1 Introduction

In the context of homeland security, one of the key challenges is achieving effective, timely and systematic collaboration and information sharing among various government agencies at the Federal, state, and local levels. Given the sensitive nature of the information, it is critical that information sharing be based on relevance and security. A majority of the agencies are using the Web as a means for sharing related information, that exists in different forms, and increasingly utilizing XML to represent this information. In case of a crisis, a virtual response team needs to be formed in an ad-hoc manner. Members of this virtual response team come from various government agencies and private organizations. Depending on several factors,

[1] This work is supported in part by the National Science Foundation under grant IIS-0306838
[2] Email:adam@cimic.rutgers.edu
[3] Email:ahmetk@cimic.rutgers.edu
[4] Email:aabhas@cimic.rutgers.edu
[5] Email:basit@cimic.rutgers.edu

doi:10.1016/j.entcs.2006.08.034

including the location and nature of the crisis, the composition of this virtual multi-agency response team may change from one crisis to another. Furthermore, during the course of a given crisis the membership of this virtual multi-agency response team (VMART) may change dynamically to accommodate various needs (e.g., public health versus fire) and to conform to certain constraints, such as jurisdictions, e.g., the crisis extends, initially from New York to New Jersey.

Members of the VMART are both information providers and consumers. As an information provider, an agency will send information, e.g., situation report, to the rest of the team as soon as it is created. As this information is "pushed" to the various agencies, there is a need to be concerned about access to this sensitive information both at the agency level (inter-agency) as well as within a given agency (intra-agency).

At the inter-agency level, each agency that is member of the VMART fulfils a certain role and, accordingly, gains access to certain information that is necessary to discharge its duties and fulfill its responsibilities within the overall efforts. For example, the public health agency would need to have access only to information related to public health, whereas FBI may need access to other related information that is different from the information needed by the public health agency. Due to the dynamic nature of the environment, a situation may arise where there is a need to admit an agency, that was not a part of the overall predefined set of agencies, as a member of the VMART. For example, as a certain crisis evolves, the Department of Homeland Security (DHS) might find it necessary to include the State Department as a member of the current VMART. In this case, DHS should be able to assign the State Department an appropriate role together with matching permissions that enable the State Department to fulfill its function in the overall efforts. Clearly, in this case, the DHS can not grant permissions, to the State Department, that they themselves do not own. At the intra-agency level, each of the agencies, that make up the VMART, has its own complex security policy. In addition, within each of these agencies there are individuals who perform a certain role (e.g., chief, first responder), possess different credentials and have different levels of access permissions that match their duties and their roles within the agency. Adherence and enforcement of these distributed policies that determine, who can access what information and at what level of granularity?, (e.g., the entire situation report, or only the part of the report that pertains to public health) are essential in order to ensure effective inter-agency and inter-governmental response. Our problem can be stated as follows. Given the environment described above, there is a need to provide each member of the VMART with automated capability to distribute to other members of the VMART only those portions of the generated information that are deemed relevant. In this paper we will limit our focus to information represented as an XML document with an underlying schema.The paper is organized as follows; section 2 discusses a motivating scenario. Section 3 provides our approach. In section 4, we detail the system architecture. Section 5 discusses related work. Section 6 includes our conclusion and future work.