Chapter 18
Design and Implementation of a Framework for Assured Information Sharing Across Organizational Boundaries

Bhavani Thuraisingham
The University of Texas at Dallas, USA

Yashaswini Harsha Kumar
The University of Texas at Dallas, USA

Latifur Khan
The University of Texas at Dallas, USA

ABSTRACT

In this chapter we have designed and developed a framework for sharing data in an assured manner in case of emergencies. We focus especially on a need to share environment. It is often required to divulge information when an emergency is flagged and then take necessary steps to handle the consequences of divulging information. This procedure involves the application of a wide range of policies to determine how much information can be divulges in case of an emergency depending on how trustworthy the requester of the information is.

INTRODUCTION

Organizations including healthcare, military, and financial have to form coalitions and collaborate to solve a particular problem such as the global war on terror or provide joint services to customers. However each organization of a coalition has to enforce policies to ensure that information is shared in a secure manner. This concept as come to be known as assured information sharing (AIS).

In our previous chapter we have described our approach to AIS. Our work was initially based on a need to know paradigm where the organizations share data according to the policies. However in many situations information has to be divulged in case of emergencies. For example, in a high security building, the building plan is not easily accessible and distributable information. But in case of an emergency such as an evacuation in case of fire, people normally unauthorized to such information are permitted to access it. For example consider a case of fire where some employees may be trapped and the building maintenance personnel are unavailable to help out. But using devices that may be able to fetch data, they may be able to use exit routes.

The work described in this chapter discusses the design and implementation of a XML-based framework for a need to share environment. In particular, we have designed and developed a Trusted Computing Base (TCB) which is essentially our framework for Assured Information Sharing that deals with the *"need-to-share"* paradigm. This paradigm shift is one of the recommendations of the 9/11 commission. This deals with dynamic environments with better flow of information. A Trusted Computing base creates a hierarchy for users of the system based on how trustworthy a user is. The level of trust can be as fine grained as possible. Based on the trust level and severity of the emergency, information is disseminated to the user.

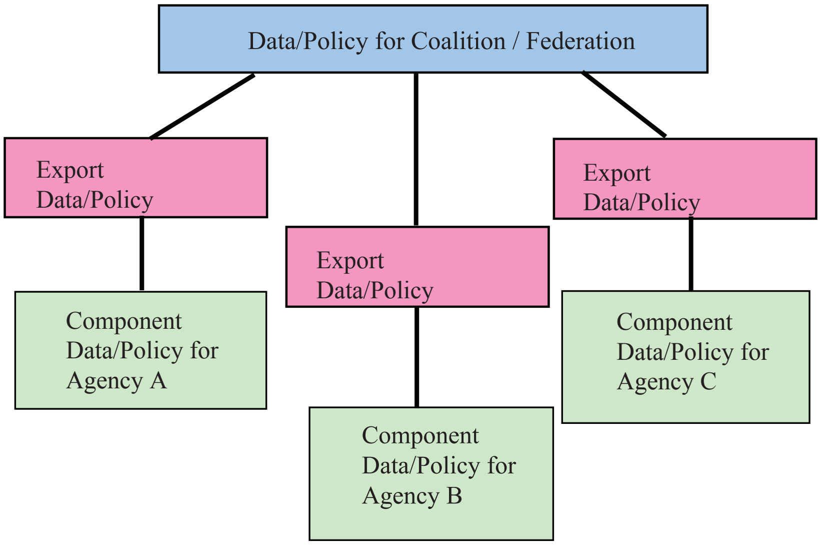
The organization of our chapter is as follows. In the Assured Information Sharing section we provide some challenges in assured information sharing including aspects of policy enforcement. The design and implementation of our prototype framework is discussed in the Design and Implementation of the Framework section. The chapter is concluded in the Summary and Directions section. The appendix consists of a set of policies that we have defined for our environment.

ASSURED INFORMATION SHARING

A coalition consists of a set of organizations, which may be agencies, universities and corporations that work together in a peer-to-peer environment to solve problems such as intelligence and military operations as well as healthcare operations. Figure 1 illustrates our architecture for a coalition where three agencies have to share data and information. Coalitions are usually dynamic in nature. That is, members may join and leave the coalitions in accordance with the policies and procedures. A challenge is to ensure the secure operation of a coalition. We assume that the members of a coalition, which are also called its partners, may be trustworthy, untrustworthy or partially (semi) trustworthy.

Security policies include policies for confidentiality, privacy, trust, release, dissemination and integrity. A broader term is dependable systems or trustworthy systems that also include real-time processing and fault tolerance. We will

Figure 1. Architecture for organizational data sharing


Data/Policy for Coalition / Federation
Export Data/Policy
Export Data/Policy
Export Data/Policy
Component Data/Policy for Agency A
Component Data/Policy for Agency B
Component Data/Policy for Agency C