



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 article 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 divulged in case of an emergency depending on how trustworthy the requester of the information is.

Keywords: Assured Information Sharing (AIS); XACML

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 article 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 article 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.

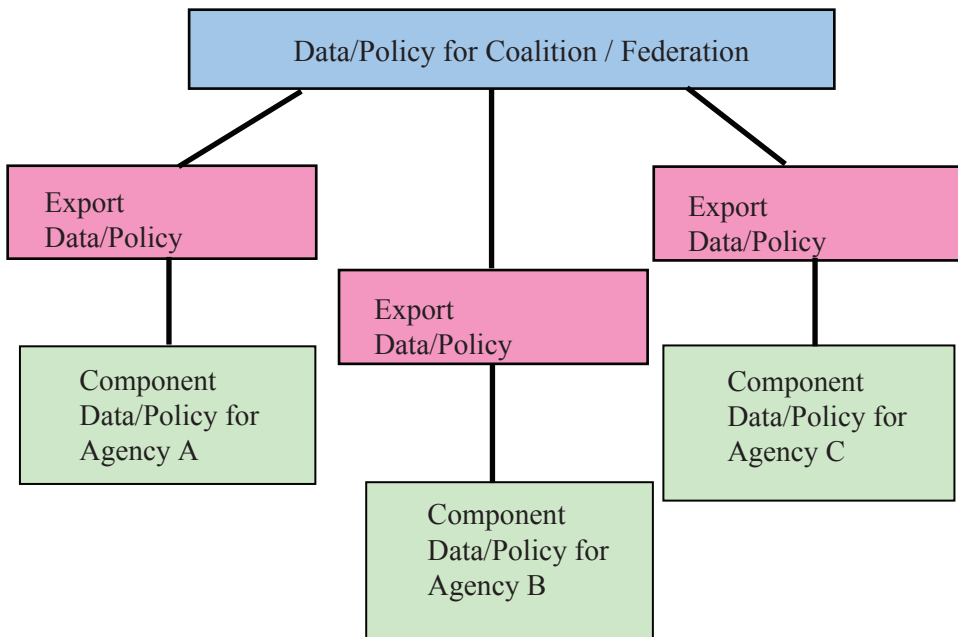
The organization of our article is as follows. In the Assured Information Sharing section we

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 article 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

Figure 1. Architecture for organizational data sharing



22 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/design-implementation-framework-assured-information/2493

Related Content

Privacy-Preserving Clustering to Uphold Business Collaboration: A Dimensionality Reduction Based Transformation Approach

Stanley R.M. Oliveira and Osmar R. Zaiane (2007). *International Journal of Information Security and Privacy* (pp. 13-36).

www.irma-international.org/article/privacy-preserving-clustering-uphold-business/2459

Security and Privacy Approaches for Wireless Local and Metropolitan Area Networks (LANs & MANs)

Giorgos Kostopoulos, Nicolas Sklavos and Odysseas Koufopavlou (2008). *Handbook of Research on Wireless Security* (pp. 732-746).

www.irma-international.org/chapter/security-privacy-approaches-wireless-local/22081

A Simulation Model of Information Systems Security

Norman Pendgraft and Mark Rounds (2007). *International Journal of Information Security and Privacy* (pp. 62-74).

www.irma-international.org/article/simulation-model-information-systems-security/2471

A Novel Approach to Develop and Deploy Preventive Measures for Different Types of DDoS Attacks

Khundrakpam Johnson Singh, Janggunlun Haokip and Usham Sanjota Chanu (2020). *International Journal of Information Security and Privacy* (pp. 1-19).

www.irma-international.org/article/a-novel-approach-to-develop-and-deploy-preventive-measures-for-different-types-of-ddos-attacks/247424

Designing a Secure Cloud Architecture: The SeCA Model

Thijs Baars and Marco Spruit (2012). *International Journal of Information Security and Privacy* (pp. 14-32).

www.irma-international.org/article/designing-secure-cloud-architecture/64344