Information Operations Across Infospheres Assured Information Sharing

Bhavani Thuraisingham and Latifur Khan
The University of Texas at Dallas

Ravi Sandhu
The University of Texas at San Antonio

Abstract of Presentation

There is a critical need for organizations to share data within and across infospheres and form coalitions so that analysts could examine the data, mine the data, and make effective decisions. Each organization could share information within its infosphere. An infosphere may consist of the data, applications and services that are needed for its operation. Organizations may share data with one another across what is called a global infosphere that spans multiple infospheres. It is critical that the war fighters get timely information. Furthermore, secure data and information sharing is an important requirement. The challenge is for data processing techniques to meet timing constraints and at the same time ensure that security is maintained. Our project addresses information operations across infospheres. The objectives of this project are as follows:

- Develop a Framework for Secure and Timely Data Sharing across Infospheres.
- Investigate Access Control and Usage Control policies for Secure Data Sharing.
- Develop innovative techniques for extracting information from trustworthy and untrustworthy partners.

The research is carried out at the University of Texas at Dallas (UTD) since December 1, 2005 with a subcontract to the University of Texas at San Antonio. We have investigated the issues and challenges for information operations across infospheres and have focused on assured information sharing. We have examined three models: In the first model the partners of the coalition are considered to be trustworthy. In the second model, the partners are semi-trustworthy. In the third model the partners are untrustworthy.

In the case of trustworthy models we conducted experiments on data sharing vs. data policy enforcement and developed a prototype system based on the concepts. Our prototype utilizes healthcare data and is based on the service oriented architecture paradigm. We have also i9bfestigated the RBAC (role-based access control), UCON (Usage control) and ABAC (Attribute based access control) models for information sharing. For the semi-trustworthy model we examined the use of game theory for extracting information from the partners. For the untrustworthy model, we have examined the use of data mining for defensive operations. In addition, we have also applied data mining techniques for Botnet detection in a Peer to Peer environment.

Our presentation will discuss the security model, algorithms as well as the prototypes we have developed for information operations across infospheres in general and assured information sharing in particular.