Analysis and Implementation of Semantic Cross-Domain Adjudication Methods

Christopher C. Lamb

May 30, 2013

Abstract

This is the abstract.

1 Introduction

Federal agencies are transitioning from a need-to-know model of information dissemination where users need to provide a demonstrative need to have access to information in order to be granted access to a more open responsibility-to-provide model. While need-to-know is being modified, it is not being removed as a requirement. Rather, agencies need to heed the notion responsibility-to-provide while still supporting robust need-to-know controls - neither can be acceptably violated in today?s environment (1). These principles affect everyone with a security clearance and all organizations that manage classified data.

These principles become difficult to rectify in today?s computational environments. The primary issue is moving classified information to an an environment at a lower classification level. This downgrading currently involves human review of data objects, in which reviewers redact sensitive information. Not all content in classified documents is necessarily sensitive, so when going through this kind of downgrading process, reviewers remove the sensitive content from the documents, leaving non-sensitive content appropriate for distribution. This process is generally referred to as sanitizing a document. This primarily impacts document downgrades, but can also impact moving information from one compartment to another, where compartments are separate categories of information within a single classification level.

This review system is an artifact of how sensitive information has traditionally been managed. To this day, computer systems are classified by the kind of information they can contain based on one of a variety of possible models. These models fall into two basic categories, government-sponsored standards or international, open standards. Current governmental standards include the Trusted Computer System Evaluation Criteria, the Information Technology Security Evaluation Criteria, and the Canadian Trusted Computer Product Evaluation Criteria. These have all been sponsored and developed by the defense

departments of the United States, Great Britian, and Canada, respectfully. The most current international standard addressing system security is thie Common Criteria, sponsored by the International Organization for Standardization. Labeled ISO/IEC 15408, the Common Criteria generalize and extend the principles established in previous, government-sponsored standards.

All of these standards group systems into categories based on security profiles that enable acceptable sensitive processing. Systems must be accredited to handle sensitive information, and the more sensitive the information, the more secure the processing system must be. This has lead to a coupling of systems and content, rather that users and content. Today, a given system is accredited to handle information of a certain sensitivity first, and then users can be granted accounts on that system giving them access to sensitive information based on an external vetting process. In this scenario, users are given access to systems, not content. Content access is a side-effect of system access.

A better approach is to evaluate suitability based on the content requested rather than the system a user is accessing. This does require a shift from current thinking, in which we accredit systems and networks for handling sensitive material to a paradigm where we evaluate each attempted access to sensitive data. In order to do this, we must have some way to describe what that sensitive data is. This implies the existence of specific ontologies that describe the information we process, as well as some mechanism to rectify them when managing content with different origins. This also implies a shift in applied security models, shifting from Bell-LaPadula and Biba models to more modern models like Brewer-Nash and Clark Wilson.

We currently envision using three different approaches and evaluating the suitability of each. The first approach is hierarchy-based, and is closest to current production systems. In this scheme, we group content based on a single tag that corresponds to a hierarchy of sensitivity. The sensitivity hierarchy is a totally ordered set, allowing us to easily make decisions about access. Though this approach is computationally simple, it does not however provide any insight into why content is classified at a particular level, nor does it support any kind of content-based access adjudication.

The second approach uses a hierarchy with attached semantic metadata attributes. Here, we maintain a totally ordered set of classifiers, but we also maintain semantic information describing specifically what it means to be grouped within one of the classifiers. This way, we can rectify content described under two different classification hierarchies. For example, if one artifact is classified under hierarchy A, and another under hierarchy B, with this additional semantic information we are able to determine specifically what it means to be classified under these hierarchies, and manage an aggregate content object formed from both artifacts more effectively.

The final approach is purely attribute based, where content and user permissions are both described with semantic information. In this case, we we no longer maintain a hierarchy of classifiers. Rather, we simply maintain semantic metadata associated with both users and artifacts, and rectify access to artifacts accordingly.