Supporting Secure Information Flow:
An Engineering Approach

Shane Bracher, SAP Research, Australia

Padmanabhan Krishnan, Bond University, Australia

ABSTRACT

The authors describe a model to provide access control for information flow that crosses organisational boundaries. The model specifies a distributed access control enforcement approach for workflow objects (e.g., a document assigned to a pre-defined workflow) using software agents and data encryption techniques. Access to restricted content within the workflow object is based on the possession of encryption keys and role enactment. The model relies on trusted software agents to verify and ensure the validity of the workflow object. The authors construct a prototype and report on a case study that demonstrates the feasibility of the proposal.

Keywords: Access Control, E-Collaboration, Information Security, Prototyping, Workflow

INTRODUCTION

As business organisations use the Internet for B2B activities, we are seeing ever-increasing amounts of data that is accessed and shared across networks spanning multiple administrative domains and organisational boundaries. Such collaborative environments pose several security concerns – for instance, risks to data confidentiality, data privacy and threats to improper data usage – leading to increased demands to address these concerns. Various authors (Biennier & Favrel, 2005; Hadaya & Pellerin, 2008) describe the issues when organisations share sensitive information with others in a business setting. Here collaboration is essential, but privacy of data is also critical. Hence the shift toward the distributed application paradigm has required a fundamental re-evaluation of information security and in particular, access control.

Of particular interest is the *loss of control* issue. When data is released into another administrative domain, the data owner relinquishes all control over it: it can be downloaded, copied, disseminated, redistributed (Miklau & Suciu, 2003). A mechanism is needed that suitably allows interested parties to maintain control over their data as it flows from one domain to another.

Consider a document that is edited and transferred amongst multiple contributors. The owner of the document might impose different restrictions on each contributor which could depend on the history of the contributions. Thus

DOI: 10.4018/jec.2012010102

the owner wishes to impose different access control requirements to the document. Maintaining control over the document's content, its structure and its flow path as it circulates through networks spanning multiple administrative domains is a non-trivial issue.

The key question we address here is how to allow the owner of logically related data items (which we call *document*) to retain control over the data after the document has been passed on to another recipient (perhaps by the owner or some other recipient). The recipient must be allowed to perform operations authorised by the owner. Furthermore, the system must be able to detect if the recipient has performed any disallowed operation. Thus we need a history (or context) sensitive access control scheme.

The principal issue of owner controlled security in a distributed environment leads us to the following questions:

- What information should be contained in the document?
- What aspects of the history are stored and where?
- What operations on the document do we support?
- How can integrity checks be performed?
- What is the role of the owner?
- How can the desired system be engineered?

This article develops an architecture model for enforcing access and change control requirements in *inter-organisational* collaborative environments. This architecture is flexible by design to allow for ease of integration within existing technology landscapes. It is developed in two phases; first as an abstract model and then a specific design of the abstract model. This design is then made more concrete into an implementation model leading to a prototype implementation and later, a pilot implementation. The use of off-the-shelf tools is a principal requirement in the implementation of our model.

ABSTRACT MODEL

Before we describe the implementation details, we present a more precise description of the problem and solution.

We will assume that we have a set of agents (A), data items (D) and operations (O). As a convenience we use the term *action* which is a data item, operation pair, i.e., an element of $D \times O$. A policy is a set of triples and a subset of $A \times D \times O$. It indicates which agents are authorised to perform which actions. This policy is dynamic in nature and can change from state to state. As usual we will have a set of states (S) to denote the evolution of the system. We defined a function *has* which given a state and a data item identifies the agent who currently has the data item. To avoid concurrency issues, we assume that only a single agent will have the data item. Similarly, the function *policy* which given a state returns the policy that is active in that state. Based on this, we can define the notion of validity of a transition. That is, a computation can move from state s to s' via the action (d,o) if $(has(d,s),d,o)$ is an element of $policy(s)$. Note that we do not define the policy that is valid in s' nor do we define who currently has the various documents. That would be left to the semantics of the implementation.

Although the policy allows the operation o to be performed on d by the agent who has access to the data item, it could also disallow other agents to perform the operation. Hence to prevent incorrect operations, the data item has to be protected. Thus the data items need to have some metadata along with the actual data. We use $d.data$ to represent the actual information associated with the data item d.

Thus the single transition at the high level can be broken down into the following steps:

1. $k = getAccess(has(d,s),d)$ which gets the access control key for d.
2. $d_a = open(k,d.data)$ which unlocks the data part of d.

Related Content

Supporting Inter-Business Collaboration via Contract Negotiation and Enactment

Peter Rittgen (2009). *Handbook of Research on Electronic Collaboration and Organizational Synergy (pp. 487-499).*
www.igi-global.com/chapter/supporting-inter-business-collaboration-via/20193?camid=4v1a