Securing XML Documents: the Author-X Project Demonstration*

Elisa Bertino
DSI-Università di Milano
Via Comelico, 39/41
20135 Milano Italy
bertino@dsi.unimi.it

Silvana Castano
DSI-Università di Milano
Via Comelico, 39/41
20135 Milano Italy
castano@dsi.unimi.it

Elena Ferrari
DSI-Università di Milano
Via Comelico, 39/41
20135 Milano Italy
ferrarie@dsi.unimi.it

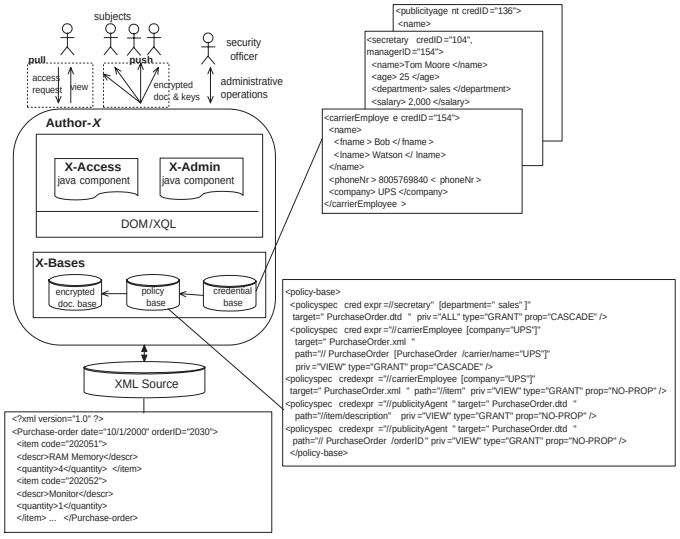

Figure 1: Architecture of the Author-$\mathcal{X}$ system

1. OVERVIEW

The widespread adoption of XML as the language for information exchange over the Web has an extensive impact on the nature of the information provided by Web sites and on the retrieval functions available to users. Such a flexibility requires adequate protection mechanisms supporting a spectrum of security requirements. The goal of this demonstration is to present the main features of the Author-$\mathcal{X}$, a system for securing XML documents, developed at the Dipartimento di Scienze dell'Informazione of the University of Milano. Author-$\mathcal{X}$ has been conceived to enforce a comprehensive protection environment for XML documents providing a variety of tools to support access control and security administration of XML documents. Author-$\mathcal{X}$ allows the specification of both *set-oriented* and *instance-oriented* security policies, by supporting DTD-level as well as document-level policies. To enforce a *differentiated protection* of XML document and DTD contents, Author-$\mathcal{X}$ security policies are fine-grained as well as positive and negative. Furthermore, Author-$\mathcal{X}$ security policies allow a *controlled propagation* of access rights. To better take into account subject profiles in the formulation of security policies, Author-$\mathcal{X}$ qualifies subjects by means of *subject credentials*. A credential is a set of properties concerning a subject that are relevant for security purposes. Subject credentials and security policies are themselves expressed in an XML-based language so that they can be adequately protected by using the protection facilities of Author-$\mathcal{X}$. Based on specified security policies, the access control tool of Author-$\mathcal{X}$ enforces both a *push distribution policy*, for document broadcast, and a *pull distribution policy*, for document release on user demand. These two policies are complementary and the choice of the dissemination mode to be adopted for a particular document is left to the Security Officer, on the basis of document characteristics and subject profiles. Author-$\mathcal{X}$ enforces also distributed document updates to enable cooperative applications over the Web. Because of the variety of access control and update functions provided by Author-$\mathcal{X}$, security administration must be adequately supported. Author-$\mathcal{X}$ provides an advanced tool environment for interactive specification, validation, and maintenance of security policies and for the management of subject credentials.

2. SYSTEM DESCRIPTION AND DEMONSTRATION

Figure 1 depicts the architecture of Author-$\mathcal{X}$. Author-$\mathcal{X}$ is built on top of the eXcelon XML data server. eXcelon manages an XMLstore where the XML data can be indexed and manipulated using the Document Object Model (DOM), and queried using the XQL language. The main focus of the Author-$\mathcal{X}$ demonstration is on selective protection and distribution of XML documents of a target XML source to be protected. The demonstration is based on the protection of an XML source in the `Supply` domain, containing documents and DTDs related to purchase orders, suppliers, clients, purchased products, and so on.

*This work has been partially supported by a grant from Microsoft Research.

ACM SIGMOD 2001 May 21-24, Santa Barbara, California, USA