Chapter XI

Protecting Datasources Over the Web: Policies, Models, and Mechanisms

Silvana Castano
Università degli Studi di Milano, Italy

Elena Ferrari
Università degli Studi dell’Insubria, Italy

ABSTRACT

Since the Web is becoming the main means of disseminating information in private and public organizations, both at internal and external levels, several applications at Internet and intranet level need mechanisms supporting a selective access to data available over the Web. Through XML, the document exchange and acquisition processes, which can be very frequent in Web-based systems, are simplified and standardized. The development of suitable security policies for both access control and information release and distribution are relevant research topics in the security field, and XML compatibility is an important requirement for Web datasource protection. This chapter covers the issues related to the definition of security policies, models and mechanisms for access control and dissemination of Web data, and is organized in two parts. In the first part, we introduce the general issues and requirements related to the definition of different types of security policies for access control and for information release in Web datasources. Then, we present security policies and mechanisms specifically devoted to the protection of XML data. In the second part, we describe the use of XML for the specification of security relevant information, focusing on security policies, subject credentials, and content protection.
INTRODUCTION

Since the Web is becoming the main means for disseminating information in private and public organizations, both at internal and external levels, several applications at Internet and intranet level need mechanisms supporting a selective access to data available over the Web. Moreover, information distribution occurs frequently in the Web context, and policies and mechanisms for a controlled release of information contents from a given source are also required. Information distribution often takes the form of documents that are made available through Web servers or are actively broadcast by Web servers to interested clients. Documents may also be exchanged among the various servers. The typical three-tier architecture for datasources over the Web consists of a Web client, network servers and the back-end information system with a suite of datasources (e.g., databases, XML sources, HTML sites) (Joshi, Aref, Ghafoor, & Spafford, 2001). Within this framework, public-key infrastructures (PKIs) (Stallings, 2000) represent an important development for addressing the security concerns of Web-based applications (e.g., for user authentication). However, these facilities do not provide mechanisms for access control to the contents of the sources, nor for their release and distribution. Protection of information sources over the Web and the development of suitable security policies for both access control and information release and distribution are relevant research topics in the security field. Security policies and related mechanisms can, in fact, be employed in several Web-based application scenarios such as digital library systems, B2B e-commerce applications, or Web-based information systems.

XML (eXtensible Markup Language) (World Wide Web Consortium, 1998) has recently emerged as being the most relevant standardization effort in the area of document representation through markup languages for Web-based information systems. Through XML, the document exchange and acquisition processes, which can be very frequent in Web-based systems, are simplified and standardized. XML compatibility is thus an important requirement for security policies, models and mechanisms for Web datasources. The widespread use of XML is emphasizing the need for models and techniques for securing XML data. These models and techniques are crucial in order to facilitate a selective dissemination of XML data containing information of different sensitivity levels, among (possibly large) user communities.

Securing XML documents entails addressing three main issues: confidentiality, integrity, and authenticity. Ensuring confidentiality means that the data object contents be disclosed only to subjects authorized according to the specified security policies. Ensuring integrity means ensuring that the object contents are not altered during transmission from the source to the intended recipient. Ensuring authenticity means that the subject receiving a data object is assured that the data object actually is from the source it claims to be. Confidentiality is ensured by access control mechanisms; integrity is usually enforced by access control mechanisms and by the use of encryption techniques, whereas authenticity requires the use of digital signature techniques (Stallings, 2000).
Related Content

Service Composition and Interaction in a SOC Middleware Supporting Separation of Concerns with Flows and Views
[www.irma-international.org/chapter/service-composition-interaction-soc-middleware/74393/](www.irma-international.org/chapter/service-composition-interaction-soc-middleware/74393/)

Fuzzy Classification in Shipwreck Scatter Analysis
[www.irma-international.org/chapter/fuzzy-classification-shipwreck-scatter-analysis/20366/](www.irma-international.org/chapter/fuzzy-classification-shipwreck-scatter-analysis/20366/)

Design Science Research: The Road Traveled and the Road That Lies Ahead
[www.irma-international.org/article/design-science-research/94541/](www.irma-international.org/article/design-science-research/94541/)

A Content-Based Approach to Medical Image Database Retrieval
[www.irma-international.org/chapter/content-based-approach-medical-image/7959/](www.irma-international.org/chapter/content-based-approach-medical-image/7959/)

Classification as Evaluation: A Framework Tailored for Ontology Building Methods
[www.irma-international.org/chapter/classification-evaluation-framework-tailored-ontology/4385/](www.irma-international.org/chapter/classification-evaluation-framework-tailored-ontology/4385/)