Chapter 3.24
Protecting Privacy Using XML, XACML, and SAML

Ed Simon
XMLsec Inc., Canada

ABSTRACT

This chapter describes how two new XML-based technologies, XACML (eXtensible Access Control Markup Language) and SAML (Security Assertion Markup Language) can be used to help protect privacy in e-services. The chapter is primarily a tutorial, briefly introducing XML, and then detailing the privacy features of XACML and SAML including XACML's ability to ensure the expressed purpose of an action matches a purpose allowed for the resource on which the action is to be performed and SAML's support for pseudonymity and communicating consent. Concepts are illustrated with detailed examples. The author hopes that readers will be both informed and intrigued by the possibilities for privacy applications made possible by XML, XACML, and SAML.

INTRODUCTION

The advent of the World Wide Web over the past decade has made it suddenly feasible for even novice human users to find and retrieve information from any Web site. Moreover, human users are not just receiving information; they are actively using the Web to carry out directives on their behalf such as ordering books, banking, and so forth.

Today, the latest Web technologies and techniques such as Web Services and Service-Oriented Architecture (SOA) herald breakthroughs for fully automatable cross-enterprise application-to-application communication, promising almost unlimited possibilities for e-services. It now becomes technically quite possible for enterprise applications (with minimal input from human users) to exchange data with each other no matter who owns them, where they are located, or what hardware and software they are made of. Rapid advances in Web technologies have eliminated what were once perceived to be natural technological barriers. But with the removal of these "natural barriers" comes the increased possibility of misuse, whether intentional or not. Advances in enabling e-services must be complemented by a technological framework that protects personal data, stipulates its appropriate use, and logs that use for subsequent audits.

This chapter gives a whirlwind tour of how new XML-based security standards, particularly XACML (eXtensible Access Control Markup Language), pronounced "ex-ack-mall" in abbreviated form, and SAML (Security Assertion Markup Language), can be used to support privacy for e-services. During the past few years since its inception, XML has become a widely used, popular format for encoding data. Many new standards for data formats are in XML for a large variety of applications ranging from document formats (such as for Microsoft Office and OpenOffice) to Web Services (enabling different computing components to work together regardless of programming language, platform, or location).

What is not so widely known about XML is that it is an incredibly useful tool for expressing and enforcing privacy policies. One of the reasons XML has become so popular is the ease with which it can be used to define and describe a data set through structure and semantics. Structure enables fine-grained dividing of data into its meaningful parts. Semantics describes what a piece of data is and can also describe how it is to be used… and describing how certain data is to be used is an important part of privacy.

BACKGROUND

This chapter starts with a gentle introduction to XML and then heads directly into a description of today's important standards relevant to those involved in assuring privacy considerations in e-services. For illustration, we introduce a fictitious scenario in which the privacy of a patient's medical record is protected using *inter alia*, an XACML policy that is evaluated dynamically according to service requests from Physicians, Administrators, and Researchers (for clarity, subject roles are capitalized throughout). Figure 1 illustrates the scenario.

In Figure 1, a user (the patient's Physician, a Hospital Administrator, or a University Researcher) wishes to view information in Patient Judy's medical record. To do so, the user signs on to the hospital's *identity and access management* (I&AM) system ([1]) and launches the appropriate application for viewing patient medical records. The application creates a service request for medical record information ([2]) that is sent to the patient medical record database. The request is intercepted by a policy enforcement point (PEP),

Figure 1. Patient medical record privacy scenario