Chapter 25
Securing XML with Role-Based Access Control:
Case Study in Health Care

Alberto De la Rosa Algarín
University of Connecticut, USA

Timoteus B. Ziminski
University of Connecticut, USA

Steven A. Demurjian
University of Connecticut, USA

Yaira K. Rivera Sánchez
University of Connecticut, USA

Robert Kuykendall
Texas State University, USA

ABSTRACT

Today's applications are often constructed by bringing together functionality from multiple systems that utilize varied technologies (e.g. application programming interfaces, Web services, cloud computing, data mining) and alternative standards (e.g. XML, RDF, OWL, JSON, etc.) for communication. Most such applications achieve interoperability via the eXtensible Markup Language (XML), the de facto document standard for information exchange in domains such as library repositories, collaborative software development, health informatics, etc. The use of a common data format facilitates exchange and interoperability across heterogeneous systems, but challenges in the aspect of security arise (e.g. sharing policies, ownership, permissions, etc.). In such situations, one key security challenge is to integrate the local security (existing systems) into a global solution for the application being constructed and deployed. In this chapter, the authors present a Role-Based Access Control (RBAC) security framework for XML, which utilizes extensions to the Unified Modeling Language (UML) to generate eXtensible Access Control Markup Language (XACML) policies that target XML schemas and instances for any application, and provides both the separation and reconciliation of local and global security policies across systems. To demonstrate the framework, they provide a case study in health care, using the XML standards Health Level Seven's (HL7) Clinical Document Architecture (CDA) and the Continuity of Care Record (CCR). These standards are utilized for the transportation of private and identifiable information between stakeholders (e.g. a hospital with an electronic health record, a clinic's electronic health record, a pharmacy system, etc.), requiring not only a high level of security but also compliance to legal

DOI: 10.4018/978-1-4666-8756-1.ch025

entities. For this reason, it is not only necessary to secure private information, but for its application to be flexible enough so that updating security policies that affect millions of documents does not incur a large monetary or computational cost; such privacy could similarly involve large banks and credit card companies that have similar information to protect to deter identity theft. The authors demonstrate the security framework with two in-house developed applications: a mobile medication management application and a medication reconciliation application. They also detail future trends that present even more challenges in providing security at global and local levels for platforms such as Microsoft HealthVault, Harvard SMART, Open mHealth, and open electronic health record systems. These platforms utilize XML, equivalent information exchange document standards (e.g., JSON), or semantically augmented structures (e.g., RDF and OWL). Even though the primary use of these platforms is in healthcare, they present a clear picture of how diverse the information exchange process can be. As a result, they represent challenges that are domain independent, thus becoming concrete examples of future trends and issues that require a robust approach towards security.

1. INTRODUCTION

Today's world is dominated by systems with a wide range of technological approaches (e.g. application programming interfaces, Web services, cloud computing, data mining, etc.), where one major objective is to support information sharing and exchange as applications are constructed as meta-systems (systems of systems), with new applications interfacing with multiple technologies, comprised of many interacting components. In such an environment, the one major challenge is to ensure that local security policies (of constituent systems) are satisfied not only when the application accesses a single system, but also when considered from a higher-level perspective. That is, an application's security is the combination of the security that must be attained within each constituent system that is accessed. What happens when security privileges of individual systems are in conflict with one another? How do we reconcile these local security policies? Is it possible to define a global encompassing security process or framework that provides a level of guarantee to the local security policies from an enforcement perspective? As today's applications continue to become more and more complex, interacting with many other systems (or applications) using varied technological paradigms, there will be a need to provide some degree of assurance that security for the application (global) satisfies the sum of the parts (local security of constituent systems). Information exchange has increased exponentially, due to the development of generic data standards (e.g., XML, JSON, RDF, OWL, etc.) and the ease of interconnection across systems, in domains such as biomedical, health informatics, library repositories, collaborative software development, etc. All of these domains present security challenges that, though not unique, have yet to be sufficiently addressed; often neither in the specific format or system (local security), and definitely not across multiple formats and meta-systems (global security).

In this effort to facilitate the intercommunication between heterogeneous systems, the *eXtensible Markup Language (XML)*[1] has become the de facto document standard for information exchange. In health care, which will serve as the case study for this chapter, XML is used for standards such as: the Health Level Seven's (HL7) Clinical Document Architecture (CDA) (Dolin, 2006) that underlies many Health Information Exchange (HIE) approaches; and, the Continuity of Care Record[2] (CCR), used for storage of administrative, patient demographics, and clinical data. In Health Information Technology (HIT), the clinical document architecture and the continuity of care