Health Insurance Portability and Accountability Act (HIPAA) Compliant Access Control Model for Web Services

Vivying S. Y. Cheng, Hong Kong University of Science and Technology (HKUST), Hong Kong
Patrick C. K. Hung, University of Ontario Institute of Technology (UOIT), Canada

ABSTRACT

Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a set of rules to be followed by health plans, doctors, hospitals, and other healthcare providers in the U.S. HIPAA privacy rules create national standards to protect individuals’ health information. Recently, there have been increasing demands and discussions about Web services-based healthcare applications. It is, therefore, necessary for HIPAA privacy rules to be standardized in Web services. However, so far no comprehensive solutions to the various privacy issues have been defined in this area. This paper summarizes the HIPAA privacy rules and surveys the topic of protecting health data privacy under the HIPAA. We propose a vocabulary-based Web services privacy framework with Role-based Access Control (RBAC) with privacy extensions and argue the HIPAA compliance for such framework. For illustration, we present the first two HIPAA rules in the extended RBAC model and embed into the HIPAA-compliant technical architecture for implementation of Web services.

Keywords: access control; health information management; healthcare information systems; healthcare infrastructure; healthcare privacy issues; privacy protection; privacy regulations; Web-enabled healthcare

INTRODUCTION

In the healthcare sector, more and more physicians, researchers, and patients are using the Internet for gathering health data (such as viewing a medical record), distributing data (for example, electronic billing) and exchanging health information (such as e-mail). For patients and doctors, accessing their health data over the Internet is becoming more popular and common throughout the world. However, with increased ease of use and access to confidential information come increased threats and vulnerabilities (Alaoui, Levine, Cleary, & Mun, 2000). With the trend of services computing, it is...
strongly believed that healthcare applications will adopt Web services technologies. A Web service is a software system designed to support interoperable application-to-application interaction over the Internet. Web services are based on a set of XML standards, such as Universal Description, Discovery and Integration (UDDI) (OASIS, 2002), Web Services Description Language (WSDL) (W3C, 2002b), and Simple Object Access Protocol (SOAP) (W3C, 2003a, 2003b).

The information exchange in a Web services-based application must be protected by privacy-enhancing technologies (Senicar, Jerman-Blazic, & Klobucar, 2003). In particular, information privacy relates to an individual’s right to determine how, when, and to what extent information about one’s self will be released to another person or to an organization (Leinonen-Kilpi et al., 2001). Information privacy is usually concerned with the confidentiality of sensitive information on the Internet. Many studies show that good privacy protection is an important factor in a well-run organization (Bennett, 1997). In general, privacy policies describe an organization’s data practices as being information they collect from individuals (consumers) and what (purposes) they use it for. There has been an increasing amount of discussion recently about a Web services privacy framework in both industry and the research community. However, so far no comprehensive solutions to the various privacy issues have been defined and developed yet. Privacy control is usually concerned with individual subjects. A subject releases his data to the custody of an enterprise while consenting to the set of purposes for which the data may be used (Fischer-Hubner, 2001). The traditional view of an access control model should be extended with an enterprise-wide privacy policy for the management and enforcement of individual privacy preferences (Powers, Ashley, & Schunter, 2002). According to the U.S. Department of Health & Human Services (HSS), the Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a set of rules to be followed by health plans, doctors, hospitals, and other healthcare providers in the U.S. (HSS, 2004). HIPAA privacy rules create national standards to protect individuals’ health information; it is, therefore, necessary to be standardized in Web services. At present, there is still no standardized Web services privacy framework for HIPAA. Thus, the importance of such a privacy framework is obvious. In particular, Cheng and Hung (2005) have proposed a vocabulary-based Web services privacy framework for tackling HIPAA compliant applications. Based on this prior work, this paper further extends and discusses the vocabulary-based Web services privacy framework of HIPAA with an extended Role-based Access Control (RBAC) model. This paper also surveys the topic in protecting health data privacy and embeds the HIPAA compliance into a proposed privacy model. The remainder of this paper is organized as follows: the next section discusses an overview of HIPAA privacy rules. The third section presents a literature review. The fourth section proposes a RBAC model apply to the vocabulary-based Web services privacy framework, whereas the final section concludes the paper with future work.

AN OVERVIEW OF HIPAA RULES

Summary of HIPAA Rules

HIPAA regulations are divided into four standards or rules: (1) privacy, (2) security, (3) identifiers, and (4) transactions and code sets (University of Miami Ethics Programs, 2005).

This paper focuses on the privacy rules in HIPAA. Under the HIPAA privacy rules, protected health information (PHI) includes individually-identifiable health information related to past, present, or future physical or mental health or condition, the provision of healthcare to an individual, or the past, present, or future payment for the provision of healthcare to an individual. The privacy rules are the most comprehensive, setting standards for how PHI “in any form or medium” should be controlled. The rules aim to ensure that organizations collect-

Copyright © 2006, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.