Chapter III

An Overview of the HIPAA-Compliant Privacy Access Control Model

Vivying S.Y. Cheng, Hong Kong University of Science and Technology, Hong Kong

Patrick C.K. Hung, University of Ontario Institute of Technology (UOIT), Canada

Abstract

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 United States of America. HIPAA privacy rules create national standards to protect individuals' health information; it is therefore necessary to create standardized solutions to tackle the various privacy issues. This chapter focuses on the e-health-care privacy issues based on a prior extension of role-based access control (RBAC) model. We review an access control enforcement model in Web services for tackling HIPAA privacy rules and protecting personal health information (PHI) called the Privacy Access Control Model. First, we discuss related backgrounds of, and privacy requirements in the HIPAA legislation. Next, four privacy-related entities (purposes, recipients, obligations, and retentions) are incorporated into the core RBAC model. The HIPAA rules are then embedded into the extended RBAC model as constraints. Then, we present a vocabulary-independent Web services privacy framework in a layered architecture for supporting healthcare applications.

Introduction

People have been concerned about health information privacy for more than two thousand years. For example, the Hippocratic Oath was written as a guideline of medical ethics for doctors in respect to a patient's health condition, and states:

Whatsoever things I see or hear concerning the life of men, in my attendance on the sick or even apart there from, which ought not to be noised abroad, I will keep silence thereon, counting such things to be sacred secrets.

It is obvious that health information is among the most sensitive and personal information that can be collected and shared. The information that needs to be protected in the healthcare sector is often referred to as personal health information (PHI). PHI includes individually identifiable health information and healthcare to an individual relating to past, present, and future physical and mental health conditions. As more and more physicians, researchers, doctors, and patients are using the Internet to access and gather their PHI, the ease of use and access to confidential information over the Internet create increased threats and vulnerabilities (Jones, Ching, & Winslett, 1995).

The principle of information privacy and disposition requires that "All persons have a fundamental right to privacy, and hence to have control over the collection, storage, access, communication, manipulation and disposition of data about themselves" (IMIA, 2001). Based on this principle, the Health Insurance Portability and Accountability Act (HIPAA) of the U.S. (2005) set a national standard to protect and enhance the right of patients to control how their health information is used and shared. Failure to comply with these legislations may lead to civil and/or criminal penalties and/or imprisonment, as well as the loss of reputation and goodwill when the non-compliance is publicized (University of Miami Ethics Programs, 2005).

To comply with the legislative requirements in the healthcare sector, access control is an essential element for limiting PHI access to legitimate users for legitimate use. The principle of access control focuses and depends on specifying requirements which are preset by the application administrator(s) or data owners. The legislation-compliant requirements can be referred to as the fundamental rules in managing those who have the right to access which PHI in the healthcare setting. In particular, the role-based access control (RBAC) model is described as more suited to healthcare than other access control mechanisms in order to meet the authorization requirements for the security of healthcare information (Ferraiolo, Kuhn, & Chandramouli, 2003; NIST, 2005). However, simply using the RBAC model is not adequate for limiting the purpose of access, storage, and disclosure of PHI.