Access Control for Healthcare

Yifeng Shen
Monash University, Australia

INTRODUCTION

Thanks to the rapid development in the field of information technology, healthcare providers rely more and more on information systems to deliver professional and administrative services. There are high demands for those information systems that provide timely and accurate patient medical information. High-quality healthcare services depend on the ability of the healthcare provider to readily access the information such as a patient's test results and treatment notes. Failure to access this information may delay diagnosis, resulting in improper treatment and rising costs (Rind et al., 1997).

Compared to paper-based patient data, computer-based patient data has more complex security requirements as more technologies are involved. One of the key drivers to systematically enhance the protection of private health information within healthcare providers is compliance with the healthcare information system security standard framework and related legislation. Security standards and legislation of the healthcare information system are critical for ensuring the confidentiality and integrity of private health information (Amatayakul, 1999). Privacy determines who should have access, what constitutes the patient's rights to confidentiality, and what constitutes inappropriate access to health records. Security is embodied in standards and technology that ensure the confidentiality of healthcare information and enable health data integrity policies to be carried out.

Based on the investigation of security standard and legislation, we can analyze and create basic security requirements for the healthcare information system. To meet the security requirements, it is necessary to deploy an appropriate access control policy and system within the organization. As discussed elsewhere (Sandhu, Coyne, Feinstein, & Youman, 1996), role-based access control (RBAC) is a promising technology for managing and enforcing security in a large-scale distributed system. In the healthcare industry, RBAC has already been adopted by the Health Level Seven (HL7) organization as a key access control standard (Blobel & Marshall, 2005).

HL7 was established in 1987 to develop standards for the electronic interchange of clinical, financial, and administrative information among independent healthcare-oriented computer systems. In June of 1994, HL7 was designated by the American National Standard Institute (ANSI) as an ANSI-accredited standards developer. HL7, in its draft Security Service Framework (Kratz et al., 2005) categorizes healthcare information security exposures in the following manner:

- **Disclosure:** Exposure, interception, inference intrusion
- **Deception:** Masquerade, falsification, repudiation
- **Disruption:** Incapacitation, corruption, obstruction
- **Usurpation:** Misappropriation

Although RBAC has been introduced to the latest version of HL7 (version 3) for strengthening the security features, it only includes those basic functions. Due to the complexity of the healthcare process, RBAC with only basic functions may not be sufficient. More context constraints need to be processed in addition to traditional RBAC operations.

The major contributions we have made in this article are:

- Illustrating the detailed design of a flexible and securer RBAC model for a healthcare information system based on HL7 standard;
- Introducing the basic elements of HL7 v3 and RBAC, which are necessary for us to realize our proposed model; and
- Analyzing the potential weakness of current HL7 standard and the basic RBAC model in terms of security and flexibility.

The rest of the article is organized as follows. The next section provides a general introduction and basic

analysis of HL7 version 3. We then explain the RBAC concept model and describe our major work, and finish with our conclusion and future work.

HL7 VERSION 3

What is HL7?

Health Level Seven is one of several American National Standards Institute-accredited Standards Developing Organizations (SDOs) operating in the healthcare arena. Most SDOs produce standards (sometimes called specifications or protocols) for a particular healthcare domain such as pharmacy, medical devices, imaging, or insurance (claims processing) transactions. HL7's domain is clinical and administrative data (HL7, 2005).

HL7 is also a non-profit volunteer organization. Its members are the providers, vendors, payers, consultants, and government groups who have an interest in the development and advancement of clinical and administrative standards for healthcare services. In its achievements so far, HL7 has already produced HL7 Version 2 (HL7 v2) specifications (HL7, 2005), which are in wide use as a messaging standard that enables disparate healthcare applications to exchange key sets of clinical and administrative data. However, the newer specification HL7 Version 3 (HL7 v3), still under development, pertains to all aspects of clinical and administrative data in health services. Unlike its older version, HL7 v3 specifications are completely based upon the extensible markup language (XML) standards, and so have potential to win an instant acceptance by developers and vendors alike.

The target system during our research is based on HL7 v3, so only HL7 v3 will be described in this article.

The lack of data and process standards between both vendor systems and the many healthcare provider organizations present a significant barrier to design application interfaces. With HL7 v3, vendors and providers will finally have a messaging standard that can provide solutions to all of their existing problems.

HL7 v3 is based on a reference information model (RIM). Although RIM is not stabilized yet, once it is stabilized, it will be the most definitive standard to date for healthcare services. The following section will highlight some key components of RIM.

Reference Information Model

RIM is the cornerstone of the HL7 Version 3 development process. An object model created as part of the Version 3 methodology, RIM is a large pictorial representation of the clinical data (domains) and identifies the lifecycle of events that a message or groups of related messages will carry. It is a shared model between all the domains and as such is the model from which all domains create their messages. RIM comprises six main classes (Beeler et al., 2005):

1. **Act:** Represents the actions that are executed and must be documented as health care is managed and provided.
2. **Participation:** Expresses the context for an act in terms such as who performed it, for whom it was done, where it was done, and so forth.
3. **Entity:** Represents the physical things and beings that are of interest to and take part in health care.
4. **Role:** Establishes the roles that entities play as they participate in health care acts.
5. **ActRelationship:** Represents the binding of one act to another, such as the relationship between an order for an observation and the observation event as it occurs.
6. **RoleLink:** Represents relationships between individual roles.

Three of these classes—Act, Entity, and Role—are further represented by a set of specialized classes or sub-types.

RIM defines all the information from which the data content of HL7 messages are drawn. It follows object-oriented modeling techniques, where the information is organized into classes that have attributes and that maintain associations with other classes. RIM also forms a shared view of the information domain used across all HL7 messages, independent of message structure.

HL7 v3 Security

The focus of HL7 security needs analysis on how systems communicate information using HL7 message. It is expected that healthcare application systems that implement HL 7 v3 will be required to have significantly more functionalities to protect the confidentiality of patient