UML Specification of e-Consent Requirements in a Health Care System

Chun Ruan
School of Computing and Mathematics
University of Western Sydney, Penrith South DC, NSW 1797 Australia
chun@scm.uws.edu.au

Abstract

Access control requirements have become an important part in any secure system. Specification of these requirements at early steps of the software life cycle can provide stakeholders rapid feedback and protect the system in a best possible way. In this paper, we utilize UML model to specify and visualize the access control policies in a health application domain. We first identify various parts necessary to specify patient record protection requirements through e-Consent, and then propose UML models to demonstrate these requirements.

1. Introduction

System analysis is an important phase in a software development lifecycle. It is important for the developers of software systems to fully understand the users' business requirements before going into the coding stage. They must understand what the system must do in order to service its purpose. A system description, or a model, is used to capture and precisely state requirements and domain knowledge so that all stakeholders may understand and agree on them. It is used to grasp conceptually what the components are

and how they interact to carry out the system functions and objectives. Stakeholders include the end users, clients, architect, analysts, programmers, project manager, and funders. The model is also used to guide the developer to explore design solutions before writing code. A model of a software system is made in a modeling language, such as the Unified Modeling Language (UML) [7]. UML is a widely accepted standard visual modeling language that is used to specify, visualize, construct, and document the artifacts of a software system. It captures decisions and understanding about systems that must be constructed.

The digital computer and information technology have changed our society, including medical society. More and more coordination of health care relies on the electronic transmission of confidential information about patients between different health care and community services. However, since the patient data is confidential, the need for electronic forms of patient consent, referred to as e-consent [2] has to be considered. Patients should be able to delegate, give or withhold `e-consent' to those who want to access their electronic health information. That is, the secure health information technology needs to support confidential patient and service provider interactions. The main application areas that need e-consent are those that support coordinated health care. This is characterized by data-sharing among multiple teams of health care professionals and institutions, and uses and disclosures of patient data. Without the existence of some e-consent mechanism, such widespread information could be accessed by unauthorized individuals, or used for purposes not originally consented to by the patient, which can lead to substantial breaches of personal privacy. By using the e-Consent, the patients are able to actively participate in the governance of the health services they need.

Access control requirements have become an important part in any secure system. Specification of these requirements at early steps of the software life cycle can provide stakeholders rapid feedback and protect the system in a best possible way. Although UML is widely used to model the software requirements, the work on UML specification for security purpose is limited. In this paper, we propose a UML model to represent security requirements regarding e-Consent in a health care application. We use use case diagrams, class diagrams and activity diagrams to visualize and demonstrate the access control requirements for electronic patient records.

The rest of the paper is organised as follows. Section 2 describes background and related work. Section 3 discusses the role-based access control model and e-Consent, while section 4 presents various aspects

978-0-7695-3428-2/08 $25.00 © 2008 IEEE
DOI 10.1109/CSA.2008.71

that are taken into account for e-Consent. Section 5 describes the proposed UML models for e-Consent. Finally section 6 concludes the paper.

2. UML and related work

The UML [7] is a de-facto standard modeling language for analysis and design of software systems issued by the Object Management Group (OMG). The primary purpose of the UML is visualizing. Its notions and diagrams provide industry standard mechanism to represent pictorially the requirements. In this paper, we use the following diagrams:

use case diagram: A use case diagram models the requirements of the system at a high level and facilitate understanding the business processes. It is used to visualize the use cases, actors and their interactions.

class diagram : A class diagram depicts the static structural aspects of an artifact being modeled. It represents properties through attributes, and behaviors through operations. Class diagrams can also show the relationships between classes, such as associations, aggregation and inheritance.

activity diagram: An activity diagram depicts the flow of activities in the system. It can model the dependency between the activities, the decision point enabling branching of the activities based on conditions specified, and the synchronization through multiple threads. It also helps in mapping the activities to corresponding actors.

There has been some research work on using UML to model the security requirements. [3] proposed a methodology to integrate the specification of access control policies into UML and provided a graph-based formal semantics. [5] presented a way to use UML 2.0 profile for secure business process modeling through activity diagrams. [6] presented a BPMN metamodel with extension that can incorporate security requirements into Business Process Diagrams. [4] showed how RBAC constraints can be specified using the object diagrams. It also showed how to use class diagrams to represent RBAC features. [1] presented the security requirements specification with UML in the context of civil aviation. Differently from their work, it this paper, we will present the requirements engineering process for security purpose in the context of e-consent in the health care domain.

3. Role-based access control and e-Consent

Classic access control is based on the individual subject accessing a resource (object).

subjects → objects

Sometimes privileges are associated with roles other than individuals. Individuals get their privileges because their roles or positions in the organization. In other words, whoever gets the role would get the privileges of the role. When people leave the organization or change the positions, their privileges will be revoked or changed, too. This happens in many organizations from the viewpoint of organization administration. Fox example, a doctor in a hospital can access the patients' information in the hospital. If the doctor leaves the hospital, he/she usually lose the capability to access the patients' information, too. If the number of subjects and objects is large, individual access control becomes difficult. Each individual needs to be assigned each access right when they get a position in the organization and revoked each access right if the person changes the role or leaves the organization. When privileges are indeed assigned to roles other than individual subjects, role-based access control can greatly simplify the administration work.

In role-based access control, roles are placed between the user and the resource and subjects get their access rights indirectly by assigning access rights to roles and roles to subjects. Roles describe rights, duties and tasks that people have to perform. When people leave or change roles, only the mapping from subjects to roles needs to be revoked or changed. On the other hand, if the duties of the roles change, only the mapping from roles to objects needs to be changed. Roles provide a more abstract viewpoint on access control.

subjects → roles → objects

The concept of role also applies to the provision of patient data in health care contexts. Some consents may be given by patients in relation to roles. For example, a patient may consent to have a pathology test done by the clinical lab staff. Multiple individuals may perform particular roles at different times, e.g. because of the need for shift-work in both intensive-care and extensive-care. Roles can be organised into hierarchies so that consents can be inherited, which could greatly reduce the amount of explicit consent specification.

4. Necessary parts for e-Consent

Dimensions of Consent

Consents may involve subjects to whom the consents are given, objects (data) to be protected, access rights allowed or prohibited on the information, and subjects who issue the consent. Consents may also be given based on purposes for the usage of data, or context of this consent. In addition, consents may be assigned for only a certain period of time.

Subjects: Roles, Individuals and Organizations

In the context of e-Consent for health care, the consent may be assigned on the basis of an individual's identity such as ``Dr Smith", or a clinical role within an organization such as Physician, or an organization such as Nepean Health Research Center. Roles can be organised into different hierarchies so that the consent can be inherited.

Objects: Patients' Data

In general, the data about a patient include: personal and contact details, clinic related details, and health details. To allow consent inheritance along the data dimension, data could be organised into hierarchies.

Access Rights

Usual access rights such as read, write, and update apply to the patient data. Access rights can also be organised into hierarchies to allow inheritance along this dimension. A consent to updating for example, may also imply a consent to reading and writing.

Consent, Denial and Delegation

Both consents and denials are needed in a flexible e-consent system. Denials are useful when patients want to express explicitly that some disclosure is forbidden. In some circumstances, a patient may wish to delegate the capability to grant consent to nominated representatives or medical practitioners, who may further wish to delegate the power to consent to other health professionals. This is usually done for flexibility, cooperation, and convenience of the carer.

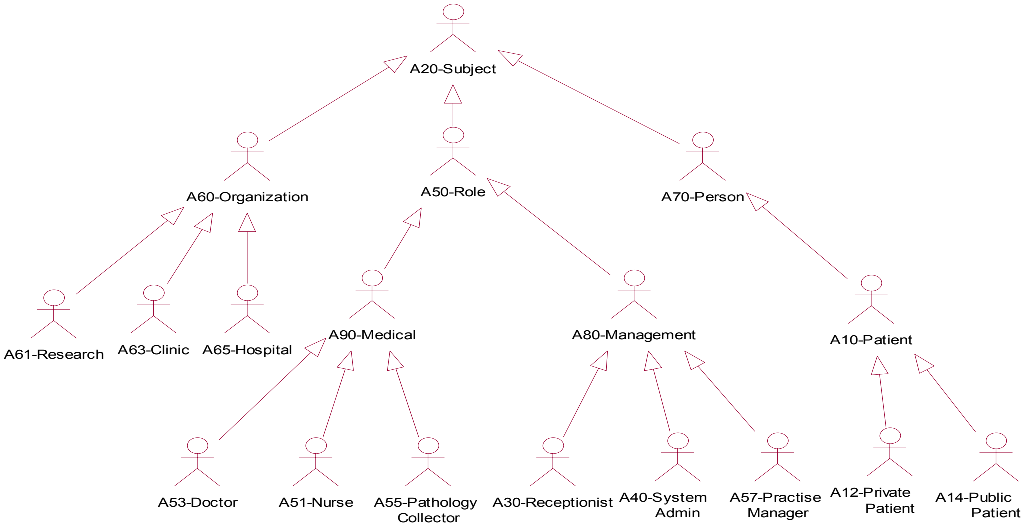

Figure 1. Role hierarchy

Conflict Resolution

Because of consent delegation, multiple grantors may exist for a specific consent and hence conflicts may arise. For example, a patient may wish to deny all information relating to HIV to be open to a research organization, but his/her family GP who has been delegated the privilege of consent granting may wish to do so. In this case, the organization may receive two conflicting authorizations, consent and denial. A proper conflict resolution policy is thus needed.

Purposes and Contexts

Sometimes, a consent is assigned on the basis of specific use of information. Common purposes include treatment, cooperation, training, teaching, notification (requests by persons closely associated with the person concerned, such as guardians, partners and immediate family), research, and getting advice from specialists.

Sometimes, consent is assigned based on the current context. A doctor may not be allowed to read the patient's health data in a normal situation, but may be allowed to do so in an emergency situation.

5. UML model for e-Consent

The access control requirements come from various sources such as domain experts and stakeholders, and it is important to represent these requirements formally in UML models.

Use case diagrams

Figure 1 shows the Actor hierarchy, which represents the users of the e-Consent system. The hierarchy reflects the inheritance relationship specified by arrows. For example, a Doctor inherits all the characteristics of a Role which again inherits all the characteristics of a Subject. Inheritance provides opportunities to reduce the complexity on the e-Consent system. For example, if some patient wishes to give consent to all medical staff in an organization, he/she only needs to give a consent to the medical role in an organization, not a consent to every specific staff. The system will automatically propagate the consent along the hierarchy.

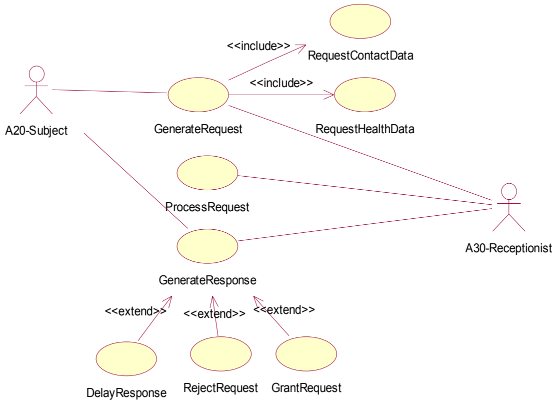

Figure 2. Use case diagram for request process

In the Request Process use case diagram as shown in Figure 2, the subject and receptionist are actors. The subject is an abstract actor that represents a patient, a role or an organization. The subject makes a request to access the patient records which include two use cases that request contact data and health data respectively. The system processes the request based on the e-Consent rules, and generates the response to the subject. There are three possible responses to generate: grant, reject or delay (undecided) denoted by three extended use cases.

In the e-Consent Maintenance use case diagram shown in Figure 3, the patient and SystemAdmin are actors involved. The use cases about creating e-Consent rules, updating e-Consent rules, and reasoning on e-Consent rules reflect major e-Consent maintenance activities. In particular, reasoning on e-Consent will need to consider consent propagation along hierarchies of subjects, objects and access rights, conflict resolution, and consent delegation.

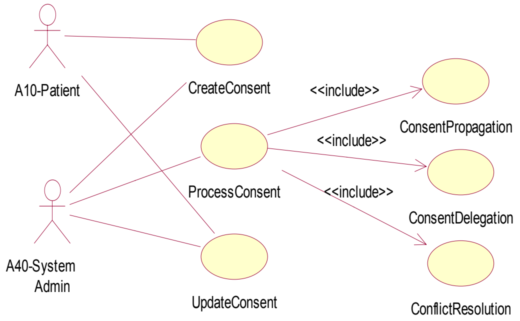

Figure 3. Use case diagram for consent maintenance

Activity diagram

Figure 4 demonstrates the access control on patient data based on the e-Consent rule system. For a request from a subject, the system generates a response based on the consent rule if it exists. Otherwise it generates a response based on the default rule (what to do by default) if it exists. Otherwise the response is undecided.

Class diagrams

Figure 5 is about e-Consent. Due to the space limit, we only show some attributes and operations for the classes Consent and PatientRecord. The class Consent is associated to subjects, patient records, access rights, types, contexts, purposes and time period. In addition, consent propagation, delegation and conflict resolution are considered in its operations.

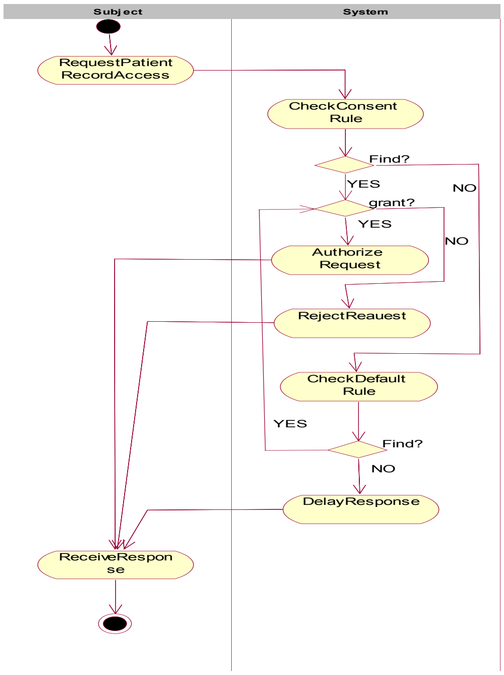

Figure 4. Activity diagram for access control

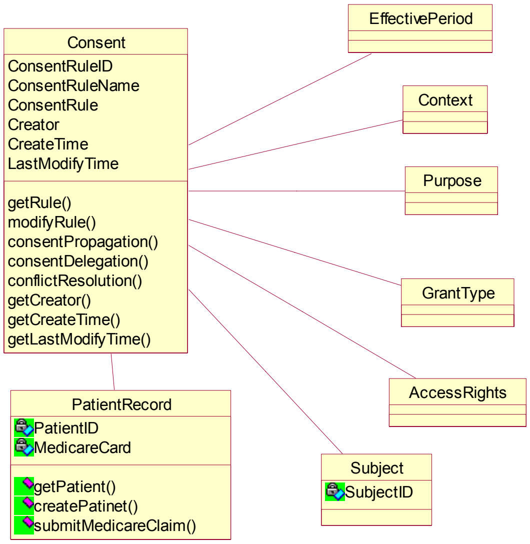

Figure 5. Class diagram for consent

Figure 6 is about patient record. The class PatientRecord inherits class Person, which has associate relationship with class ContactData. The PatientRecord is an aggregation of classes Consultation and HealthData. Also, the PrivatePatient inherits the attributes and operations of the class Patient.

Figure 7 is about subject. The class Subject is a generalization of classes Role, Person and Organization, which have association relationships with each other.

6. Conclusion

In this paper, we have shown how patient requirements regarding health information protection using e-Consent can be specified in UML models. One of the main benefits of the approach has been to raise all access control issues regarding patients' records at the analysis stage of software development process. This enables better communication to stakeholders and reduces the risk of delivering a system that does not meet patients' security needs. For the future work, we will extend and enrich the security requirements specifications using UML. We will also investigate automated code generation for security from the UML model.

6. References

[1] R. Darimont and M. Lemoine, Security requirements for civil aviation with UML and goal orientation. LNCS 4542, 2007, pp. 292-299.

[2] E. Coiera, e-Consent: The Design and Implementation of Consumer Consent Mechanisms in an Electronic Environment. *Journal of the American Medical Informatics Association*, 11 (2004), pp. 129-140.

[3] M. Koch, F. Parisi-Presicce, UML specification of access control policies and their formal verification. *Software System Model,* 5 (2006), pp. 429-447.

[4] I. Ray et al, Using UML to visualize role-based access control constraints. *SACMAT*, 2004, pp. 115-123.

[5] A. Rodriguez, E. Fernandez-Medina, M. Piattini, Security requirement with a UML 2.0 profile. In *Proc. of the First International Conference on Availability, Reliability and Security*, 2006, pp. 670-677.

[6] A. Rodriguez et al, A BPMN extension for the modeling of security requirements in business processes. IEICE *Trans. Inf.& Syst*. 4 (2007), pp. 745-752.

[7] J. Rumbaugh, I. Jacobson, G. Booch, *The Unified Modeling Language Reference Manual*, Addison-Wesley Publishing Company, 2005.

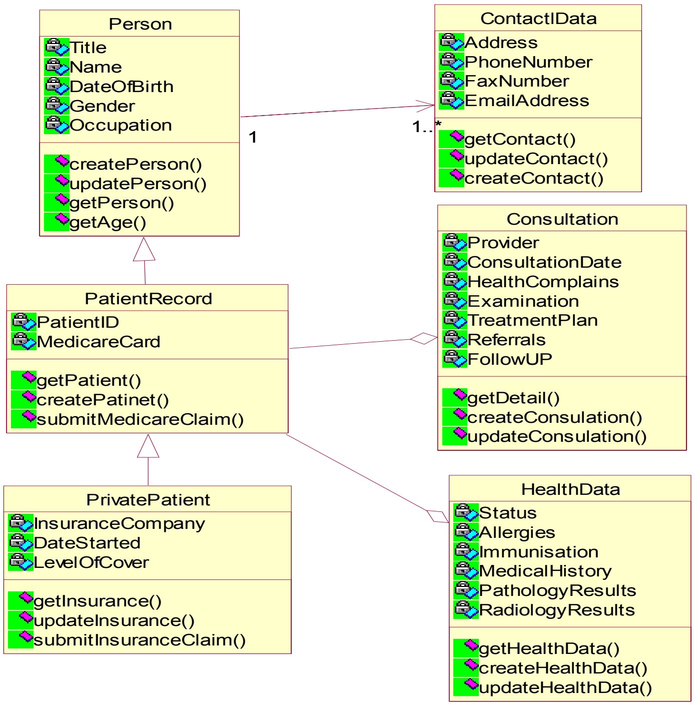

Figure 6. Class diagram for patient record

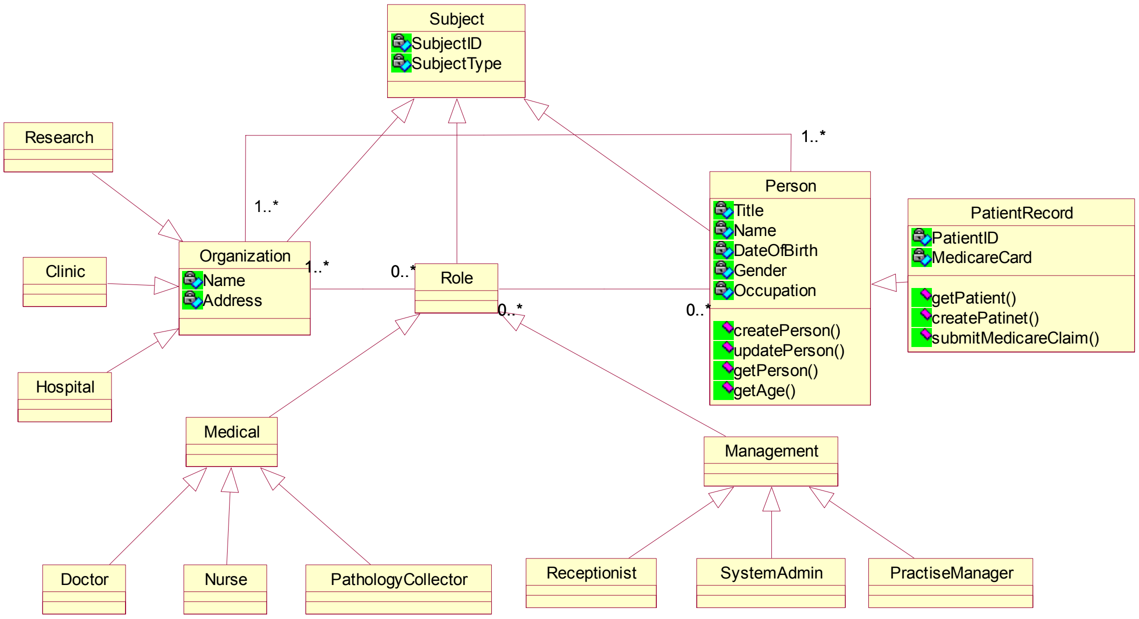

Figure 7. Class diagram for subject