MEDINFO 2007
HISA Ltd Australia
© 2007 The authors. All rights reserved.

MG-RBAC: Using Medical Guidelines as a Source of Contextual Information to Activate and Deactivate Roles and Permissions

Lillian Røstad[a]

[a]*Department of Computer and Information Science, Norwegian University of Science and Technology, Norway*

Abstract

Controlling access to information is a key concern in healthcare systems. Some form of Role-Based Access Control (RBAC) is implemented in most healthcare systems. A problem with existing RBAC models used in healthcare is their static nature which doesn't capture the dynamic needs of healthcare providers. In this paper we propose an enhanced access control model combining RBAC with the use of Medical Guidelines, MG-RBAC. Medical guidelines contain temporal and contextual information that may be used to make more informed, dynamic access control decisions.

Keywords:

access to information, computer security, privacy

Introduction

Access control is a key concern in healthcare systems. In order to ensure privacy of patient data, the systems has to provide suitable mechanisms to control access to information. Many existing healthcare systems use some form of Role-Based Access Control (RBAC) Ferraiolo D.F., Kuhn D.R., Chandramouli R., Role-Based Access Control, Artech House Publishers, 2003, ISBN 1-58053-370-1. . Access decisions are typically based on a user's role (e.g. nurse, medical doctor etc) and workplace (department, ward). A user is granted access according to his/her role's permissions for patients that are admitted the ward where he/she is working.

However, these static properties are often incapable of capturing the dynamic needs of healthcare personnel. In this paper, present a model for using Medical Guidelines (MG) as a source of information for access control decisions as a way of creating more dynamic access control for healthcare.

MGs (or clinical practice guidelines) are defined by Field M.J, Lohr K.N., Clinical Practice Guidelines: Directions for a New Program, The National Academy of Sciences, 1990. as:

"Practice guidelines are systematically developed statements to assist practitioner and patient decisions about appropriate health care for specific circumstances."

There exist several formalized notations for computer-interpretable MGs. MGs may include temporal and event information that implies information needs and therefore may be used in access control.

Computer-interpretable medical guidelines

The Asbru MG notation has been chosen as the notational example used in this paper because it contains constructs for defining periodic and event-triggered clinical tasks that suits our demonstration needs, and because Asbru MGs are encoded in XML (eXtensible Markup Langua[1]ge) which is a widely used format for exchange of data.

The Asbru Language

Asbru is a time-oriented, intention-based, skeletal plan-specification representation language [3]. A skeletal plan specified in Asbru consists of a name and a plan body and may additionally contain (optional): a set of arguments, a time annotation, preferences, intentions, conditions and effects. The plan body contains a set of plans (child plans) and information about how/in which order these plans should be executed and also conditions on which child plans must be completed in order to complete the parent plan.

An example MG in Asbru

An example of use of Asbru for encoding a guideline for treatment and observation of Gestational Diabetes Mellitus (GDM – a form of diabetes found in pregnant women) is available at [3]. Use of the guideline is initiated if a glucose tolerance test in the third trimester shows a blood sugar level between 140 and 200 mg/dl. The guideline consists of three main parts:

- Glucose monitoring: measurements performed by the patient herself and/or by the physician. Check to verify that glucose level kept below a limit of 130 mg/dl for 1-hour post meals, < 100 mg/dl fasting and preprandial.
- Nutrition: treatment is based on teaching patient a diet. The goal is to manage GDM with diet and without insulin therapy for as long as possible. Regular follow-ups (every 1-4 weeks) are recommended.

1 http://www.w3.org/XML/

- Insulin therapy: initiated if blood sugar consistently > 100 mg/dl fasting and/or one hour postprandial consistently higher that 130 mg/dl and attempts at diet modification has failed.

MG-RBAC

The Asbru guideline for GDM contains both temporal and contextual information that may be used for access control:

- Periodic information needs: visits to physician while under treatment every 1-4 weeks (specific value set for a patient). The EPR does not need to be accessible to the physician in-between visits.
- Events that trigger information needs: when blood sugar readings are too high the patient needs to visit her physician and review treatment. The EPR should be made accessible to the physician when too high readings occur.

A few UML use cases have been created to illustrate the envisioned use of medical guidelines in access control for healthcare systems.

Periodic consultations are part of the guideline for GDM. Even if the physician is regularly seeing the patient he/she does not need access to the EPR at all times. The physician might need to prepare for an appointment and enter some information after the appointment, but it should be sufficient for the EPR to be accessible e.g. two days prior to and two days past the next scheduled visit for a patient. Figure 3 - Guideline: periodic access3 illustrates how this may be done. The physician will have an assigned role that includes permissions to this patient's EPR as he has a responsibility for this patient. But this role is only activated around a scheduled visit.

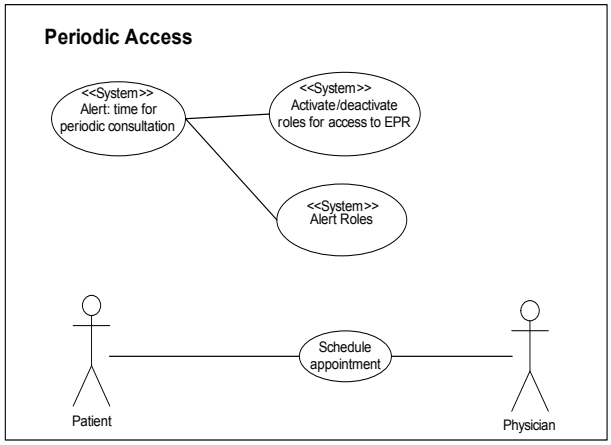

Figure 3 - Guideline: periodic access

The other example of use of guideline information for access control decisions is the occurrence of events that trigger information needs. A typical example of such an event is a measurement of some sorts, made manually or by a sensor, which triggers further actions. For the GDM example the glucose monitoring illustrates such an event. The patient is to measure her own blood sugar level 4 times a day. If the measured level is above some specified limit further action needs to be taken. To determine further actions the physician needs access to the patient's EPR. Figure 4 - Guideline: event trigger4 illustrates how roles are activated if the guideline specifies that a measure results in an action that requires access to the EPR and the relevant role (or roles) is activated.

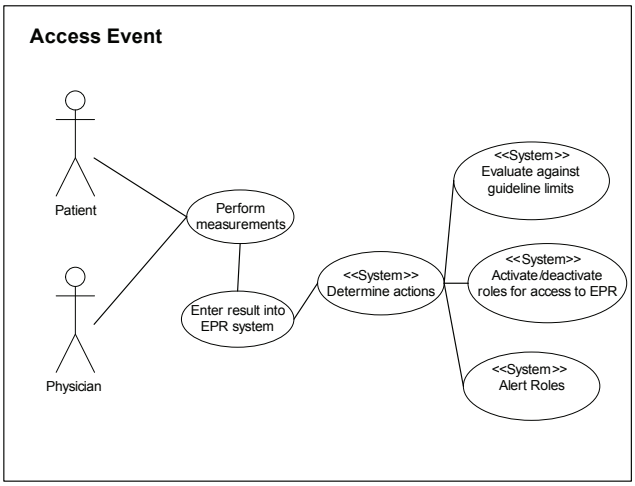

Figure 4 - Guideline: event trigger

Discussion

The model presented here for MG-RBAC is only very preliminary and serves to inform about a promising idea that requires further work.

The examples presented are based on a guideline representation in the Asbru language. Certainly for such a model to be useful it should be able to use guidelines in many different notations. One possible solution would be to integrate a guideline translation engine in the Guideline Monitor module. Work remains as to examine in details information contained in other guideline specification languages and how they may be translated.

The examples presented here only illustrate triggered and periodic events. There may be additional information contained in guidelines that could be utilized in access control, but this has not been fully explored yet.

Conclusion and future work

In this paper we have presented an idea and a preliminary model for using medical guidelines as input to access control. The idea is that guidelines contain information that can assist in creating a dynamic and context aware access control model for healthcare.

We intend to continue to explore this idea further by creating a more detailed model and developing a proof-of-concept implementation.

References

[1] Field M.J, Lohr K.N., Clinical Practice Guidelines: Directions for a New Program, The National Academy of Sciences, 1990.

[2] Ferraiolo D.F., Kuhn D.R., Chandramouli R., Role-Based Access Control, Artech House Publishers, 2003, ISBN 1-58053-370-1.

[3] The Asgaard Project, http://www.asgaard.tuwien.ac.at (last accessed: December 2006).