Towards Dynamic Access Control for Healthcare Information Systems

Lillian RØSTAD, Øystein NYTRØ

"Department of Computer and Information Science, Norwegian University of Science and Technology, Trondheim, Norway

Abstract. Access control is a key feature of healthcare information systems to protect the privacy of patients and to ensure access to information as required by healthcare professionals. A problem with many existing access control mechanisms is their static nature. In this paper we propose combining workflow information from medical guidelines, observations and audit logs to create dynamic access rules that are adapted to the actual workings of a hospital. Our aim is to help minimize the use of “break the glass” access.

Keywords. Security, Data protection, Evidence based guidelines

Introduction

Access control is one of the key features of health care systems. Access control is about restricting as well as ensuring access to information. These are two inherently different viewpoints. For privacy it is important that access is only granted when there is a legitimate need. For availability it is equally (some would argue more) important that access is granted to all information required to provide the best possible care. The goal of the work presented here is to narrow the gap between these viewpoints, by proposing a method for dynamic access control rules that adheres to the actual flow of work and responsibilities in a hospital setting.

1. Access Control Concepts

Access control is about enforcing rules on which operations a user is allowed to perform on a resource (e.g., information) in a system. There are several different access control models. The most common ones are mandatory access control (MAC), discretionary access control (DAC), and role-based access control (RBAC) [1]. RBAC is the preferred model used in many implemented access control mechanisms in health care systems and serves as the foundation for the ideas presented here.
1.1. Role Based Access Control

The concept of Role Based Access Control [1] has gained increasing popularity over the last decade. In RBAC a set of roles is created that corresponds to job functions in an organisation. Each role consists of a set of access rules. Rather than assigning access rules directly to a user, a user is linked to the role and thus has all the access rules associated with that role. Several users may be assigned to the same role, and one user may take more than one role. A typical RBAC role in a health care system would be that of a nurse. The nurse role consists of access rules that correspond to the information access a nurse needs to perform his job.

The main advantages of RBAC are ease of administration, flexibility, and scalability. RBAC is considered a good fit when there are considerably fewer roles than employees in an organisation. When a new nurse is hired there is no need to create a specific access profile for him – he can simply be assigned to the existing nurse role. This scales well as it is easy to add more nurses as an organisation grows, and it is flexible because changing the access rules for all nurses only requires changing one role.

Some health care systems [2] combine a role with the user’s place of work to make access decisions. In short, this means that a nurse only has access to users that are currently admitted to the ward where he works. Dynamic RBAC is extended to assign roles temporarily, according to work shifts or work processes.

1.2. Optimistic Security

In [3] Povey proposes the concept of optimistic security. The key feature in an optimistic security mechanism is the use of retrospective control. There are no access rules that are enforced when a request is made. The concept relies on the ability of someone to examine the logs later and determine if the access was legitimate. Auditing and traceability therefore are keys to enforcing optimistic security. Povey argues that optimistic security is well suited for systems such as healthcare where there may be situations when a user needs to exceed his normal privileges.

Optimistic security exists in many healthcare systems as a “break the glass” mechanism intended to be used in emergency situations. A study [2] has looked into use of the “break the glass” mechanism in a system where normal access control is enforced as a combination of role and workplace as explained earlier. In the study audit data was collected for one month’s use of the system at eight hospitals. The study found that 54% of the patients admitted in this time period had their record accessed using the “break the glass” mechanism. Out of all accesses made in this period, 17% were performed using the “break the glass” mechanism. These findings strongly suggest that the rather static approach to access rules (role and ward) does not perform very well in a dynamic hospital setting.

The 17% accesses resulted in almost 300 000 entries in the audit logs. The study also found that there were no automatic audit analysis tools in place. The amount of audit trails and the absence of tools make the task of analyzing audit trails for retrospective control impossible. A condition for optimistic security to work, is that the amount of use is minimal so manual review is realistic.

In health care there will always be situations where availability of information is crucial and “break the glass” mechanisms are needed. One example is emergency situations when there is no time to properly register the patient in the administrative
systems, which often is a requirement for normal access rules to apply. The goal is therefore not to completely eliminate the use of “break the glass”, but to reduce the use to an amount where it is feasible to perform retrospective control. One approach towards this goal is developing access control mechanisms that are better adapted to the actual workings of a hospital and are dynamic in the sense that they are able to change and adapt as situation and context change. We will explore this idea further in this paper.

1.3. Dynamic access control – related work

As stated earlier, a problem with many access control rules in health care is the “define once – use always” approach and the lack of dynamic properties and adaptability. Several extensions to RBAC have been proposed to include dynamic properties. Examples include role delegation [4] and context-sensitivity [5]. Role delegation allows a user to delegate her role to another user to transfer responsibilities either permanently or time-limited. In the proposed context-sensitive RBAC models, context is used to activate and deactivate roles. A user may have a large pool of assigned roles and only a subset of these may be activated at any given time. Context properties may be used to regulate the activation of a role. E.g info about work schedule may be used to activate roles depending on time and place of work.

Though some propositions have been made on how to make RBAC more dynamic, a discussion of exactly what properties or values may be used remains. In the remainder of this paper we propose combining established best practices (medical guidelines), collected observational data, and audit data to learn patterns of information used in healthcare and apply these patterns to create access control rules that will help minimise use of «break the glass» access.

2. Workflow knowledge

Medical guidelines, work plans, observed behaviour, and audit data all contain information about workflow in healthcare. While medical guidelines are the idealised version of the medical activities related to a problem, observational and audit data reflects what actually happens [6]. Moreover, guidelines do seldom assign roles or resources. However, by combining these sources of knowledge we can create a coherent view of enacted workflows in healthcare, with an emphasis on information access requirements that may be utilized for access control.

In this section we discuss medical guidelines, observation data and audit logs separately and provide motivational examples of how this information may be used for access control purposes.

2.1. Medical Guidelines

A medical guideline (MG) for a given diagnosis contains information about best practice course of treatment developed by experts in the field. Guidelines may exist both as an informal collection of information and in a more formalised, structured manner. MGs often include temporal and event information that implies information needs that may be utilized for access control purposes.
An example of a guideline for treatment and observation of Gestational Diabetes Mellitus (GDM – a form of diabetes found in pregnant women), encoded in the Asbru language for computer-interpretable medical guidelines, is available at [7]. 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, nutrition, and insulin therapy.

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 patient record should be made accessible to the physician when too high readings occur.

2.2. Observational data – empirical grounding of guidelines

Guidelines are constructed by experts and represent idealized treatment processes – what is expected to happen given a diagnosis. In reality, each patient and care process is unique; furthermore, a complex problem will require that different guidelines are combined. A guideline may serve as a starting point, but will often need to be adapted to the specific situation at hand. In [6] the authors discussed how to use methodical observations of clinical care situations to improve guideline implementation.

An observational study was carried out in the summer of 2005. Two medical students observed clinicians at work in the pre-rounds meeting and ward rounds. They took detailed notes of who were present, the subject of discussion (patient), information sources (written/electronic and oral), and specifics about what type of information was used. In each observation session they followed one clinician and from her viewpoint they noted who else were present and what role they had in the situation. We have reviewed these data to construct an example of how observational data may be used to create patterns of information needs, shown in Figure 1.

Due to space limitations, Figure 1 shows only the first few interactions in the pre-visit meeting, but it is sufficient to serve our purpose as an illustrative example. In this case they are discussing patient NN. The patient is new to the doctor so the nurse fills him in on some background info. Several information sources are used – some are paper-based (the patient list and the patient chart) and some are computer-based information systems (the electronic patient record (EPR) and the radiology imaging system (IDS)). The figure illustrates communicative acts between the actors present and the actors and the information sources they use. Roles are used to label the actors. This figure illustrates how observation may be used to uncover information needs in specific situations with a specific diagnosis (in this case heart failure), and link these to roles. Though not shown in Figure 1, the observational data shows that the diagnosis changes as test are being done and test results received and reviewed, as is very common. Through observational studies we can examine these transitions and study transfer of responsibilities and access requirements related to this.
Even if observations provide real-world examples that may be collected over time, generalized, and used to improve guidelines, they still only give us a relatively high-level view. To complete this picture and get detailed and accurate information about information accessed and actions performed, we turn to the audit logs.

2.3. Usage patterns from audit logs

Most health care systems keep complete history; of changes in information and of user actions. The purpose is to always be able to roll back to a previous state, and to have complete traceability. This means that there exist audit logs with very detailed traces of user actions: the user’s role at the time, what information was accessed, for which patient and what actions were performed [2]. From these audit logs it is possible to create generalized usage patterns per role. If a system allows “break the glass” access, it is also common to require the user to provide a reason for doing so and keep a log of these reasons as well [2]. We suggest utilizing this information for access control by:

1. Examine the reasons for using “break the glass” – any reasons that occur often should be considered as candidates for inclusion in the access control rule set.
2. Look for common usage patterns that describe workflows inwards. Examples include:
   - **Temporal patterns**
     - If action X occurs – then action Y occurs within Z time.
   - **Responsibility patterns**
     - If action X is performed by Role A – then action Y is performed by role B.
   - **Location patterns**
     - If action X is performed at ward 1 – then action Y is performed at ward 2.
   - **Situation patterns**
     - Role X is in situation S in a guideline, and requires specific information.
3. Discussion

“Break the glass” access is necessary to handle unexpected situations, but it constitutes a security risk and may be misused. The ideas presented here aim at minimizing the need for glass-breaking and making retrospective control feasible.

In access control, the main concern is privacy, where access should only be granted to the information required by an actor in any situation. Clinicians may well disagree with this from the viewpoint that it is better to have broad access. In this paper we therefore suggest an approach to access control that combines guidelines and learning from observations and logs. The goal is to take another step towards the goal of having access mechanisms that support the work of care providers, while protecting the privacy of patients.

The approach presented here is not another “do once – use forever approach”. It is fundamental to this idea that observing, learning, and improving should be a continuous process, allowing access rules to adapt to a dynamic, ever-changing environment.

4. Conclusion and future work

In any clinical situation, the information about a patient can be ordered along a continuum from highly relevant, via interesting, to irrelevant, and at the other extreme; illegal according to laws of privacy. Being able to sort correctly may mean life and death. The main problem facing today’s busy clinician is avoiding irrelevant information and at the same time getting access to relevant information. In this perspective, relevance ranking and access control depend on the same knowledge about situation, role, guideline, and care process. We believe that optimistic access control, based on analysis and learning from practice as intended and as enacted, is a first step towards both effective relevance ranking and optimal access control.

References