

## Dynamic, Intelligent and Adaptable Access Control

Lillian Røstad, Gunnar René Øie, Øystein Nytrø  
{lilliaro, gunnarre, nytroe}@idi.ntnu.no  
Norwegian University of Science and Technology  
Department of Computer and Information Science  
<http://www.idi.ntnu.no>

Access control is a key feature in most healthcare systems. There is a need to balance availability of information for the caretakers, while protecting the patient's right to privacy that can only be solved with a well-suited access control regime. A problem with many existing access control models implemented in healthcare systems is their static nature. At the core of this problem is the attempt to guess information needs at design-time, while leaving little ability for dynamic changes at runtime. Indeed this is true also for systems in many other domains than healthcare.

Some form of Role-Based Access Control (RBAC) [1] is commonly used for access control in healthcare systems. A set of roles (doctor, nurse etc) are defined and assigned to users. A role is a set of permissions corresponding to the assumed access needs of users assigned to this role. However not all possible situations and information needs can be predicted. This is true for emergency situations when the patient has not been entered into the system as admitted, and therefore no one has access. But there are also situations such as requests for second opinions, transfer of patients and responsibilities when dynamic changes in access rules are necessary. As a result most healthcare systems include a "break the glass" mechanism that allows caretakers to override the access rules in such situations. The use of this mechanism is supposed to be infrequent, and auditing of access logs is supposed to be used in retrospect to make sure that accesses made are legitimate. However, a study [1] of use of one such mechanism over a one-month period showed that:

- 74% of the users had the permission to use this mechanism.
- 54 % of the patients had their information accessed using this mechanism.
- 17 % of all accesses were performed using this mechanism.

17 % out of a total of 1 794 153 lookups in the study period means there are 297 742 entries in the access log that should be examined to determine if they are legitimate.

In our work we focus on developing access models that incorporate contextual information to make informed, dynamic access decisions. At the heart of this approach is identifying workflow patterns, and creating a system that is able to adapt as workflow patterns change over time. Initially we have identified three candidate sources of contextual, workflow-related information that may be utilized in making access decisions: medical guidelines, audit data and data from observation of healthcare personnel interacting with patients and systems.

### ***Medical guidelines***

Medical guidelines (or clinical practice guidelines) are defined by [3] as:

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

In other words a medical guideline for a given diagnose contain information about best-practice course of treatment developed by experts in the field. A medical guideline may include temporal and event information that implies information needs and therefore may be used in access control. An example is the medical guideline for treatment and observation of Gestational Diabetes Mellitus (GDM – a form of diabetes found in pregnant women) [4]. This

guideline specifies that the patient should monitor her glucose level. If the measured value exceeds a limit the doctor should review the patient's information and an appointment may be necessary. This guideline also specifies periodic visits to the doctor. This information may be used to grant the doctor access when the next visit is approaching, or when a glucose measurement exceeds the limit.

### ***Audit data***

Information written to system logs can be a valuable source of information on how the users actually use the system. It reflects the actual use of the system, not how one thinks the system will be used. In health care system one is required to keep complete history, and provide transparency of use of information to patients, and therefore very detailed logs are kept. This information can be a basis for improving the access control rules. One can discover simple access patterns such as which documents are most commonly access by which users or roles. More complex temporal patterns may also be discovered by looking at audit data. An example may be a pattern showing that after a doctor accesses a patient's record, a nurse at the same ward access a specific part of the record within a few hours.

### ***Workflow data from observation***

Actual usage patterns may also be discovered by observing healthcare personnel at work. A large amount of observation data has been collected including information on what information is required by which roles to perform specific care tasks. This is valuable information for access control.

Our goal is to create a dynamic access control engine that utilizes information from these three sources, and potentially more, to make informed, dynamic access decisions. The information sources may be updated, manually with observation data or automatic for audit data, which enables the access control system to adapt as system context changes.

## **References**

- [1] Ferraiolo D.F., Kuhn D.R., Chandramouli R., Role-Based Access Control, Artech House Publishers, 2003, ISBN 1-58053-370-1.
- [2] Røstad L., Edsberg O., A Study of Access Control Requirements for Healthcare Systems Based on Audit Trails from Access Logs, In Proceedings of the Annual Computer Security Applications Conference (ACSAC), Miami, 2006.
- [3] Field M.J, Lohr K.N., Clinical Practice Guidelines: Directions for a New Program, The National Academy of Sciences, 1990.
- [4] The Asgaard Project, <http://www.asgaard.tuwien.ac.at>.