Requirements for Access Control: US Healthcare Domain

Konstantin Beznosov
Baptist Health Systems of South Florida
6855 Red Road, Coral Gables, FL 33143
beznosov@baptisthealth.net

The differences in the requirements of disclosing patient information from state to state, the diversity in healthcare providers' business models, the increased rate of merges, and the upcoming federal regulations in healthcare make access control requirements a moving target for application developers and healthcare enterprise designers and administrators. We suggest two major design principles for access control infrastructure deployed in the healthcare enterprises: isolation of the application logic from the authorization logic and centralized administration of the authorization logic.

Application systems and healthcare enterprises constructed according to these two principles will be able to accommodate changes in access control logic and will enforce a uniform access control model across an enterprise. However, the complexity and instability of the healthcare access control model makes the task of applying these design principles somewhat difficult. The notion of roles and their hierarchies help to alleviate complexity of controlling access to patient data, but it has to be used in conjunction with other information, such as affiliation, relationship, location and so on.

We identified the following factors that have to be used to make elaborate authorization decisions in order to comply with patient information discloser requirements:

Affiliation – what subsidiary of the health system a particular caregiver works for. Due to frequent mergers and to the fact that many physicians consult in several hospitals, this factor affects the authorization decision.

Role – what role the user is assigned to during the current session. This factor is important to use because the same user can act in different roles performing his or her responsibilities and because role-based access control decreases security administration overhead. However, access control policies show us that the type of relationship between the user and the patient is used more frequently in making authorization decisions.

Location – where the user is accessing information services from. Location information is used in several types of authorization rules. One type is represented by the following example of an access control policy: a nurse should have access to medical records of a patient if the nurse is currently working on the same "floor" as the patient. Another type uses location to identify the trust domain where the user is accessing information services from. A reasonable policy would deny access to any sensitive information to anyone accessing it from such areas. Location can also be used to derive the emergency level of access. A policy can allow read access to all patient information of all patients for any user assigned to the role physician and accessing the information from an emergency room.

Time The time factor is useful for authorization rules on users assigned to shift-related positions such as nurses and for team-based access control.

Relationship – what is the relationship between the user and the patient whose records are to be accessed. Some types of relationships that need to be managed in the healthcare context are: patient's primary care provider; admitting, attending, referring, or consulting physician of a particular patient; part of the patient care team; healthcare staff explicitly assigned to take care of the patient; patient's immediate family; patient's legal counsel or guard; personal pastoral care provider.

Roles are important factors in authorization rules. However, other information is essential in order to make authorization decisions at healthcare enterprises. An effective authorization language that would incorporate concepts of roles, affiliation, location, relationships and time is needed.