SitBACReasoner: Reasoning about access-control situations with OWL
Dizza Beimel¹, PhD, Mor Peleg², PhD
¹Department of Industrial Engineering and Management, Ruppin Academic Center, Israel;
²Department of Management Information systems, University of Haifa, Israel;

Abstract. Healthcare providers need to access Electronic Health Records (EHR) in order to provide adequate patient care. At the same time, the patients’ privacy should not be compromised. Based on extensive qualitative studies, we have previously defined Situation-Based Access Control (SitBAC) – a conceptual model for representing context-based healthcare access-control policies. We implemented a prototype mechanism for determining the policy that applies to a given access-control request using an OWL ontology of access situations and a reasoner that classifies incoming access requests into access situations.

Background. Private data may be protected by access-control mechanisms. SitBAC is a conceptual model for representing context-based access-control (AC) policies that we developed following an extensive qualitative study that elicited AC scenarios. SitBAC structures access-request scenarios into situations of AC in which defined relationships hold among the following entities and their properties: Patient, Data-Requestor, EHR, Task, Legal-Authorization, and Response. The access requests include reading patient data or recording clinical actions in the EHR. For example, in Fig. 1, a nurse is allowed to document the nursing-section and to view the medication section of patients hospitalized in her department, while she is working her shift.

Methods. The Ontology Web Language (OWL, www.w3.org/TR/owl-features/) is a description logics language used to define ontologies for sharing information over the web. We implemented the SitBAC model as an OWL ontology using Protégé (protégé.stanford.edu). We used Semantic Web Rule Language (www.w3.org/Submission/SWRL/) to infer composite relationships between properties (e.g., the patient’s location is equal to the data requestor’s department), and used the Pellet reasoner to classify data access requests (represented as ontology instances).

Results. (1) The ontology’s main concept is Situation, which defines the entities participating in an AC scenario and their possible properties and relationships. Situation is specialized into specific defined situation subclasses whose Response entity is a necessary condition. This enables the reasoner to classify a situation instance into its corresponding situation subclass and infer its Response type (approved or denied). Fig. 1 shows the definition of the NurseInPatient situation subclass.

We designed the knowledge-base of situations to be minimal, complete, and non-conflicting, taking advantage of ontology exception patterns and using the reasoner to discover potential duplications.

Discussion. Other researchers have used OWL for representing AC policies. As in those approaches, a reasoner is used to maintain a consistent ontology. Our approach differs in that we use a reasoner to classify an incoming AC request instance into one of the AC situation classes. However, the exponential time-complexity of the reasoner is a limitation which needs to be considered in future work.

Figure 1. the implementation of SitBAC model as OWL ontology using Protégé 2000

References