Reasoning about access-control situations with OWL

Dizza Beimel[1], PhD, Mor Peleg[2,3], Tim Redmond[2]

[1]Department of Industrial Engineering and Management, Ruppin Academic Center, Israel;

[2]Department of Management Information systems, University of Haifa, Israel;

[3]Center for Biomedical Informatics Research, Stanford University, Stanford, CA;

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. Private data may be protected by access-control mechanisms. 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. SitBAC[1] 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.

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*[2] reasoner to classify data access requests (represented as ontology instances).

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. Fig. 1 shows the definition of the NurseInPatient situation subclass.

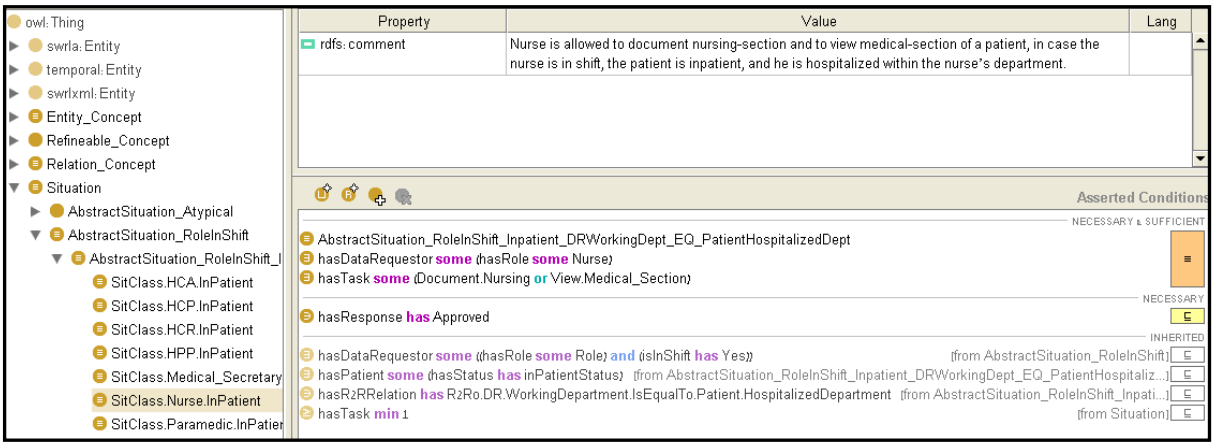

Figure 1. a Situation subclass from the OWL ontology, defined using Protégé

Closing the ontology's classes and individuals enabled us to perform closed-world reasoning. Using the Pellet reasoned, we realized situation individuals into their corresponding situation subclass and inferred their Response type (approved or denied).

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.

Other researchers have used OWL for representing AC policies[3,4]. 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.

References

1. M. Peleg, D. Beimel, D. Dori, and Y. Denekamp. Situation-Based Access Control: privacy management via modeling of patient data access scenarios. J Biomed Inform, available online 10 April 2008, doi:10.1016/j.jbi.2008.03.014 2008.
2. E. Sirin, B. Parsia, B.C. Grau, A. Kalyanpur, Y. Katz. Pellet: A Practical OWL-DL Reasoner. Web Semantics: Science, Services and Agents on the World Wide Web 2005;5(2):51-3
3. J. Bradshaw, A. Uszok, R. Jeffers, N. Suri, P. Hayes, M. Burstein, et al. Representation and Reasoning for DAML-Based Policy and Domain Services in KAoS and Nomads. In: Intl Conf Autonomous Agents; 2003.
4. T. Finin, A. Joshi, L. Kagal, J. Niu, R. Sandhu, W.H. Winsborough, et al. ROWLBAC - Representing Role Based Access Control in OWL. In: Proc 13th Symposium on Access control Models and Technologies; 2008; 2008. p. 73-82.