Modelling a User Authorisation and Data Access Framework for Multi-specialty Research Systems in Secondary Health Care

Ire Ogunsina[1], Sarah N. Lim Choi Keung[1], Lei Zhao[1], Gavin Langford [3], Edward Tyler[1], and Theodoros N. Arvanitis[2]

[1] Department of Primary Care Clinical Sciences
[2] School of Electronic, Electrical and Computer Engineering
University of Birmingham, Edgbaston, Birmingham B15 2TT, United Kingdom
[3] Birmingham and Black Country Comprehensive Local Research Network
{i.ogunsina,s.n.limchoikeung, l.zhao, e.tyler, t.arvanitis}@bham.ac.uk, Gavin.Langford@uhb.nhs.uk

Abstract. Patient identification and consequent recruitment in clinical trials is normally preceded with searches on electronic health record (EHR) systems. Query results may be collated across multiple health organisations and specialties. In such scenarios, a prime concern is the possibility of systems and their users inadvertently or otherwise impinging on the privacy of patients. Access to patient data is crucial for research purposes, but the degree of access must be controlled in such a way that it conforms to agreed legal, organisational and ethical policies. In this paper, we present a proposed model for managing a dynamic matrix of roles and data access privileges within the context of research systems in secondary care.

Keywords: Role Based Access Control (RBAC), secondary care research, electronic healthcare records.

1 Introduction

Patient data is arguably the most essential resource in health care systems. The recommendations of the Caldicott guardian stipulate that access to patient data must strictly be on a "need-to-know" basis [1]. Caldicott-compliant systems need to be effective in granting and restricting access to patient data and resources according to system and user specifications. This work is part of a larger project involved with the design and development of a research system to be used for clinical studies across multiple specialties in secondary care. System users (subsequently referred to as the subjects) will typically be health practitioners with proficiency in at least one specialty and affiliated to one or more health organisations, typically NHS Trusts.

Apart from the patient data resource, license protected resources also exist for the computation of clinical data. Access to all resources need to be verified along several lines to ascertain rights and permissions. The paper continues with an overview of the

P. Kostkova, M. Szomszor, and D. Fowler (Eds.): eHealth 2011, LNICST 91, pp. 105–108, 2012.

classic RBAC, some known limitations and possible solutions. Sections 3 and 4 focus on the context of our work, the reasoning and rationale behind the proposed model.

2 Overview of the Traditional RBAC

Originally proposed by Sandhu [2], RBAC is a standard of access control whose popularity is proof of its effectiveness. RBAC is based on a grouping mechanism, known as roles. A subject's role, therefore, determines what resources they have access to. This approach breaks the tight coupling between the subject and the permissions to resources. From a data modelling perspective, the inclusion of the role entity resolves the many-to-many relationships between subject and rights or access to resources [3]. Within the health enterprise, the effectiveness and appropriateness of the RBAC approach as a privileges management infrastructure has been successfully demonstrated by Slevin and Macfie [4].

2.1 Problems

Although RBAC has proven its effectiveness and good utilisation record across a wide industrial spectrum, the approach is not to be considered as a panacea for all access control issues [2]. The traditional RBAC has been shown to have limitations, making it unsuitable for scenarios requiring complex access requirements [5]. Some of the main problems, often associated with RBAC, are related to potential policy conflicts and inconsistencies with authorisation of subjects with multiple roles. The objective of our work is to model an effective framework for granting or denying access requests to patient data and resources. This framework must take into consideration the combination of the roles, specialties, Trusts, resources and actions requested. The scope of the proposed model does not include more challenging scenarios, such as emergency access requests.

3 Making Access Decisions

3.1 Policies

Multiple role assignments to a subject can potentially contribute to the problem of separation of duty and role precedence [5]. Our approach lends from the PERMIS authorization infrastructure project [6] where the subject, for example, is an object which could have an attribute-key, role with the attribute-value, researcher-only, or an attribute-key first_name, where the attribute-value may be Fred. The proposed model is also a policy driven model where access criteria are contained in separate policies. *Trust policies* for instance, would exist to specify the different relevant directives that may exist for the subject within the context of their affiliation with the health organisation. Similarly, *specialty policies* exist to provide directives relating to subject specialties that could influence the access decision. By default, each attribute has its policy. Our model contains an access decision framework, which provides a decision based on the aggregation of the different policies.

3.2 Resources

Apart from patient data, another requirement of the model is the management of system resources and tools. An example is licensed quality of life questionnaires which may exist in paper or electronic format. A typical case is the Hospital Anxiety and Depression Scale (HADS) [7] score in the COPD specialty. These licenses are usually bought by the Trust and used in calculating patient data.

The RBAC model of the now defunct NHS National Programme for IT (NPfIT) project [8] includes additional concepts for suitability within the health enterprise. Within each policy entity, directives would specify the concept status such as *Legitimate Relationships (LR)* - ensuring that patient identifiable data is only accessible if the subject is involved in the patient's care. Non patient identifiable data may be accessed as allowed within the *Sealed Envelopes (SE)* segments of policy documents. In most access request scenarios, it would be impossible to be granted access without *Patient Consent (PC)* status being true within policy documents.

As shown in Figure 1, the scalable model generates a decision outcome as a product of aggregated policies. This approach gleans from Blobel's more detailed model [9] as well as HL7's security policy information model [10].

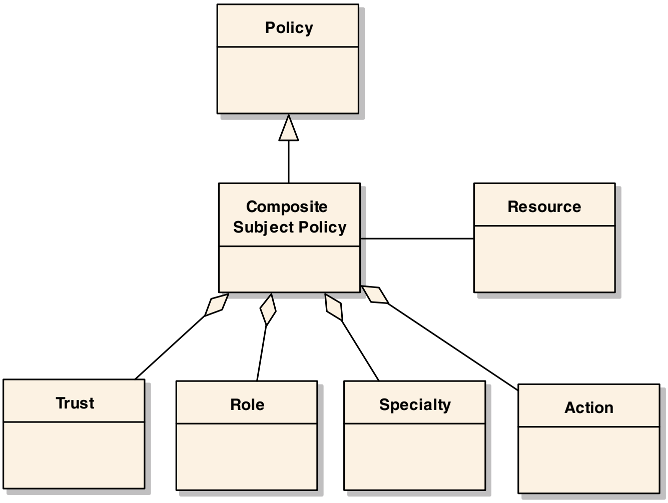

Fig. 1. Policy-based model for resource access decisions

4 Conclusion and Related Work

4.1 Related Work

Farzad and Yu [11] extended Crook's RBAC model [12] which modelled the concepts of responsibility, operation and context in addition to the role concept as criteria for object access and permission, bears good resemblance with our approach work described with particular focus on including the model during the knowledge engineering phase. Although the work by Slevin and Macfie [4] involves a single specialty and Trust in a clinical environment, it highlights challenges common to access control mechanisms within healthcare systems and possible solutions.

4.2 Conclusions and Future Work

Traditional RBAC may be extended to include policies and constraints that will augment its suitability in complex scenarios. Our proposed model is a policy-oriented framework which handles access decisions in a flexible way within the context of multi-specialty research systems in secondary health care. It would be beneficial to see how integrating Cassandra, [1] a role based, trust management system into the permissions management infrastructure would facilitate our model. Furthermore, it would be interesting to research on aligning our model fully with the HL7's Privacy, Access and Security Services (PASS) Access Control Services model [10].

Acknowledgements. The work was supported by the England's National Institute for Health Research (NIHR) and the Birmingham and Black Country Comprehensive Local Research Network (BBC CLRN).

References

[1] Becker, M.Y., Sewell, P.: Cassandra: Flexible Trust Management, Applied to Electronic Health Records. In: Computer Security Foundations Workshop, pp. 139—154 (2004)

[2] Sandu, R.S., Coyne, E.J., Feinstein, H.L., Youman, C.E.: Role-Based Access Control Models. IEEE Computer 29, 38–47 (1996)

[3] Ferraiolo, D.F., Kuhn, D.R.: Role Based Access Controls. In: 15th National Computer Security Conference, pp. 554–563 (1992)

[4] Slevin, L.A., Macfie A.: Role Based Access Control for a Medical Database. In: IASTED-Software Engineering and Applications Conference, pp. 19–21 (2007)

[5] Covington, M.J., Moyer, M.J., Ahamad, M.: Generalized Role-Based Access Control for Securing Future Applications. Technical Report GIT-CC-00-02. Georgia Institute of Technology (2000)

[6] PERMIS. FAQ (2011), http://sec.cs.kent.ac.uk/permis/documents/FAQ.shtml

[7] Snaith, R.P.: The Hospital Anxiety and Depression Scale. Health Qual. Life Outcomes 1, 29 (2003)

[8] National programme for IT (NPfIT), http://www.gpchoice.org/npfit.aspx

[9] Blobel, B.: Authorisation and Access Control for Electronic Health Record Systems. International Journal of Medical Informatics 73, 251–257 (2004)

[10] HL7. Privacy, Access and Security Services (PASS) Access Control Services Conceptual Model. Release 1 (2010), http://hssp-security.wikispaces.com/PASS+HL7+Balloted+Documents

[11] Farzad, F., Yu, E., Hung, P.C.K.: Role Based Access Control Requirements Model with Purpose Extension. In: Workshop on Requirements Engineering, pp. 207–216 (2007)

[12] Crook, R., Ince, D., Nuseibeh, B.: Modelling Access Policies Using Roles in Requirements Engineering. Information and Software Technology 45(14), 979–991 (2003)