COORDINATING POLICY FOR FEDERATED APPLICATIONS

Ken Moody
University of Cambridge Computer Laboratory
New Museum Site, Pembroke Street
Cambridge CB2 3QG, UK
km@cl.cam.ac.uk

Abstract At the start of its present term of office in 1997 the UK government published a planning document promising ubiquitous access to Electronic Health Records (EHRs) held within the National Health Service (NHS). If such access is to become a reality then it is essential to guarantee confidentiality, since otherwise the media and the privacy vigilantes will prevent deployment. Among the rights included in the Patients' Charter is a promise that each individual may determine who may access their health records and in what circumstances, and that every access made shall be logged. In October 1999 the Cambridge Computer Laboratory's Opera group joined a consortium within the Eastern Regional Health Authority to propose an experimental architecture that included access control. Policy governing access to a particular set of records is derived from many high-level sources, and must be updated when any of these sources change. We outline an architecture to achieve this, within the framework of access control policy for EHRs. The problems of coordinating policy arise in many applications that span management regimes, and the techniques outlined are more generally relevant. This is work in progress.

1. Introduction

The thrust of the Opera group in the Computer Laboratory has been to develop a Middleware architecture in which individual services retain autonomy. Key components are the Cambridge Event Architecture (CEA) [8], which offers support for generic registration and notification of events, and the role-based access control model Oasis [5]. These components are interdependent. An overview of the work of the Opera group can be found in [1].

It is one thing to propose an architecture for distributed applications, quite another to evaluate such an architecture realistically. In Oasis role names are defined and policies expressed on a service-by-service basis, so providing for independent management of the individual services involved. It is therefore possible to deploy policy while respecting the autonomy of management domains, enabling complex wide-area applications to evolve without fine-grained coordination. In April 1999 members of the Opera group visited the Information Authority of the UK National Health Service (NHS), and the group has since developed a detailed architecture to support ubiquitous access to EHRs, including role-based access control. We have learnt a lot from carrying out the design, but we should learn a lot more by testing it in practice.

2. Electronic Health Records: a Federated Management Problem

The UK NHS has been underfunded over a long period, and is recognized as being in crisis. The Labour government that took office in 1997 made reviving the NHS one of its prime goals [12]. [13] outlined an implementation strategy intended to lead progressively to the integrated storage of health data, with access from all health care points. The strategy was based on bottom-up deployment, and there was no clear explanation of the mechanisms that would ensure compatibility across the country as a whole. The Opera group joined a consortium (EREHRC) formed by health care providers within the Eastern Region, coordinated by the Clinical and Biomedical Computing Unit (part of the University of Cambridge), based at Addenbrooke's Hospital. The EREHRC included health professionals and academics based within the region and from outside, among them Jane Grimson of Trinity College, Dublin, who led the European Community *Synapses* project [10]. In November 1999 the EREHRC submitted a proposal to the NHS for a "pan-community demonstrator", focussing on what we see as the main obstacles to the introduction of EHRs: heterogeneity, local autonomy, and above all continuing evolution - of hardware and software, management structures, and medical practice and taxonomy.

The EREHRC proposal contained a separate technical appendix developed by the Opera group, together with a sabbatical visitor, John Hine, from the Victoria University of Wellington, New Zealand. Specific proposals for a certificate authority suitable for supporting Oasis in a health care environment are described in [6]. An overview of the architecture is given in Figure 1.

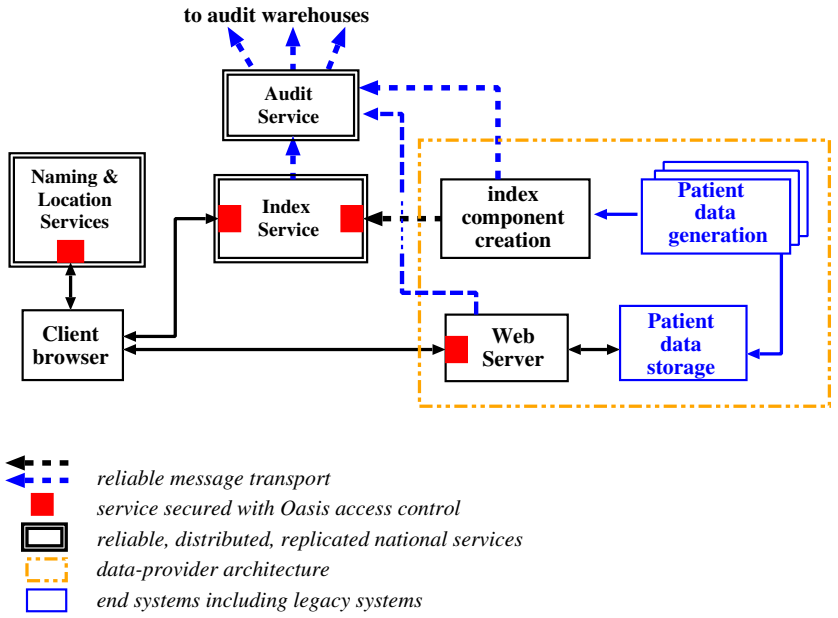

Figure 1. An Architecture for an Electronic Health Record Service

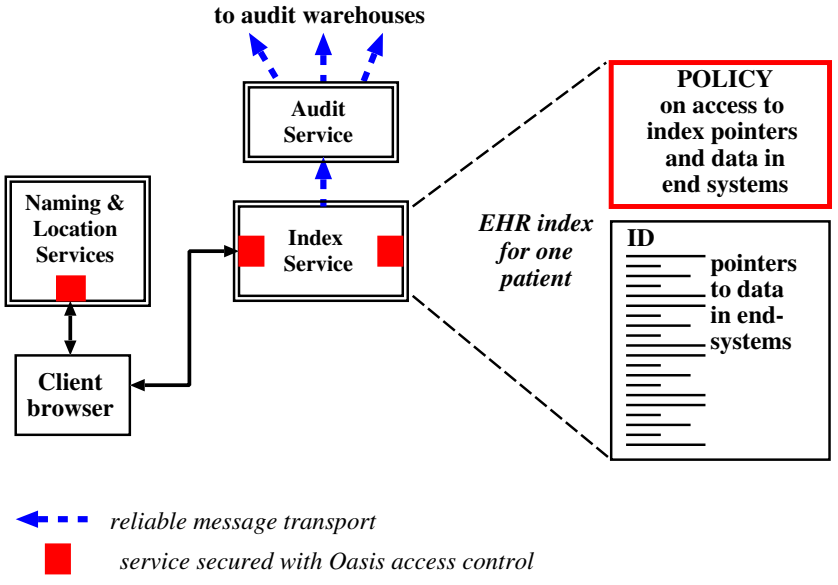

Figure 2. The Virtual Health Record (Index) Service

A crucial feature of the design is the use of virtual health records [3, 4], essentially index items structured according to a medical ontology. Each such item contains references to all the patient records relating to a given individual, see Figure 2. By law every access to an individual's EHR must be recorded, and we provide an audit trail asynchronously, noting the principal reading the data, and the context. This context must include information sufficient to identify the policy regime that was current at the time of access, together with the credentials presented by the principal in order to establish the right to access the data.

NHS thinking at that time was based on solutions involving a centralised database, and the proposal was not funded. Public opinion has remained critical of the NHS, and after wide consultation the Labour government presented a new national plan for the health service in July 2000 [14]. There is little emphasis on ubiquitous access to EHRs, and the implementation strategy introduced in [13] has been quietly forgotten.

3. The requirements for managing access control policy

Access to an individual's EHR is regulated in a variety of ways. In particular, EHRs must be identified, and they contain personal data; EHRs are therefore subject to Data Protection legislation, as enacted in both the UK and European parliaments. The Health Service is administered independently in England, Wales, Scotland and Northern Ireland, and each province has established its own Patient's Charter [11]. Amongst other things, each charter makes explicit each patient's right to determine who may access their health records. Health authorities will express policies in terms of the role and seniority of their staff, and the nature of the data that is to be accessed or service that is to be managed. Specialist departments will recognize professional skills in addition to seniority. All of these sources of policy must be respected when generating procedures (Java classes, in our case) to implement the access control guards on databases which contain patient records. For each high-level source non-specialists should be able to express policy intuitively, in a language appropriate to the context. The large scale of an application such as the NHS means that guards on the individual databases must be generated automatically. Audit records must identify the policy regime under which each access has been authorised.

4. Oasis Role-Based Access Control

In Oasis each named role is associated with a particular service. A service that administers roles is responsible for authenticating its clients.

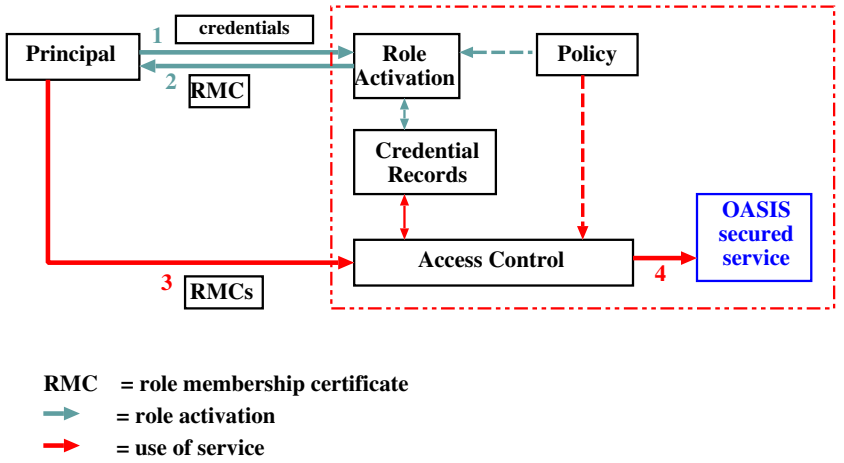

Figure 3. A service secured by Oasis access control

Rights to access a service are derived from membership of roles, either of the service itself or of other services. Figure 3 shows a service secured by Oasis access control. Policy is checked both on role activation and when the service is used.

A client becomes authenticated in a particular role by presenting credentials that enable the service to **prove** that the client conforms to its policy for activating that role, see [9] which describes the formal model. The credentials presented can include parameters that are checked during role activation. The client is then issued with a role membership certificate (RMC). The RMC may include parameters derived from the credentials that identify aspects of the client, for example a local user identifier may be copied from a log-in certificate; a digital signature is generated to protect the parameter values and to ensure that the certificate is useless if stolen.

Services authorise clients by specifying the privileges associated with each role. The policy may require parameter values to satisfy constraints which must be checked whenever access is attempted.

Role-based access control (RBAC) has a number of advantages. Permissions are expressed in terms of roles that may be adopted by principals. The policy governing role activation is decoupled from the rights associated with each role, which may be modified at a generic level. This leads to essentially scalable policy management, and incidentally enables secure access by anonymous principals, should this be desired.

A crucial practical advantage of making roles specific to a service is that each service may specify its own policy for both role activation and access control. In an environment such as a hospital it is likely that a central registry service will act as the sole certificate issuing authority [6], with individual hospital departments granting access on the basis of the RMCs that have been issued. Policy within each hospital will determine role membership hospital wide; once an appropriate policy has been expressed, any departmental service can control access on the basis of the RMCs issued by the central registry service. In this way both hospitals and individual departments can be managed independently; Oasis access control can thus be deployed incrementally. This is vital in any application that comprises a federation of independent partners.

5. Expressing and enforcing policy

In the NHS application access control must respect both individual preference and hospital policy. The former is determined at the index service, the latter by guards established at each departmental patient record service. A student on the MPhil course in Computer Speech and Language Processing has defined a simple formal language for policy expression [7, 2]. Successive translations generate Higher Order Logic, First Order Predicate Calculus (FOPC), and finally target languages specific to both Role Activation and Method Invocation (including data access). Basic RBAC will not handle the negative permissions that patients may require, but in Oasis role activation conditions can also include environmental constraints [9]. Examples of such constraints are to check on the time of day, or to evaluate a predicate in a local database. Since parameters such as a local user identifier may be set during role activation it is possible to handle patient preferences by consulting a list of exceptions in some appropriate database.

The use of environmental constraints makes it possible to define generic policies that can be tailored to each particular context. We are at present setting up mappings between the names of predicates which express environmental constraints and the names of database relations. For example, a software package for primary health care can specify default policy using role-based access control. Any exceptions requested by individual patients can be handled by consulting a locally maintained database, provided that names are handled consistently from practice to practice. Additional policy expression languages will be needed, but they will also generate FOPC. It is vital to establish a common target representation in order to check the overall consistency of policies.

6. Managing change

The high bandwidth and reliability of modern communications make it inevitable that applications will be federated across a wide area, with individual management domains interacting subject to a high-level regulatory framework. In the NHS application each of the four home countries has its own Patient's Charter, and the access control policy effective when health care is delivered must take account of the appropriate version. Throughout the UK any policy must respect the provisions of the Data Protection Act.

For the NHS EHR application we have implemented active database support that should help us to automate policy deployment. The policy effective at a health care point may derive from a number of sources; national law, regulatory frameworks such as the Patient's Charter, local health authority access control policy and individual patient preference. Any inconsistencies must be identified and resolved before deployment. We are storing each such policy in an object-relational database, setting triggers to alert all sites dependent on it whenever a change occurs. What action is taken will vary from site to site. If no inconsistency results then it should be possible to deploy a modified policy automatically, otherwise local management must decide how to resolve the conflict. Many problems remain to be solved before automatic enforcement of expressed policy can become a reality.

7. Risks of automated policy enforcement

An essential feature of the EREHRC architecture is that change can be managed locally, with national decisions being implemented on a time scale that is feasible within each environment. Policy is only one of many sources of change. The structure of EHRs must be modified in the light of medical research; advances in genetics are now threatening the simplistic view of individual patient preference, as genetic counsellors are confronted more and more frequently with differences of opinion between siblings - the sister wishes to know the result of a test, but the brother does not. This raises a dilemma. As the scale of electronic health data increases it will become essential to automate the capture of both data and policy, yet the computer is insensitive at best in matters such as ethics.

Business to business dealings between multinationals are subject to even worse problems; not only must contracts be interpreted within a variety of legal frameworks, but any disputes arising may be subject to multiple jurisdictions. In such a world there is a real danger of unstable behaviour, with a consequent threat to secure economic growth.

Acknowledgements

We acknowledge EPSRC's support for the continuation of this work under GR /N35786 "Access Control Policy Management".

References

[1] Bacon, J., Moody, K., Bates, J., Hayton, R., Ma, C., McNeil, A., Seidel, O., and Spiteri, M.: Generic Support for Asynchronous, Secure Distributed Applications. IEEE Computer Vol. 33(3), 68–76, March 2000

[2] Bacon, J., Lloyd, M and Moody, K.: Translating role-based access control policy within context. To appear in Policy 2001, Workshop on Policies for Distributed Systems and Networks, Bristol, UK, January 2001. Lecture Notes in Computer Science 1995, Springer-Verlag, Berlin, Heidelberg and New York, 105–117, 2001

[3] Grimson, J., Felton, E., Stephens, G., Grimson, W. and Berry, D.: Interoperability issues in sharing electronic healthcare records - the Synapses approach. Proceedings of Third IEEE International Conference on Engineering of Complex Computer Systems, IEEE CS Press, Los Alamitos, Calif., 180–185, 1997

[4] Grimson, J., Grimson, W., Berry, D., Kalra, D., Toussaint, P. and Weier, O.: A CORBA-based integration of distributed electronic healthcare records using the Synapses approach. Special Issue of IEEE Transactions on Information Technology in Biomedicine on EMERGING HEALTH TELEMATICS APPLICATIONS IN EUROPE, Vol.2, No.3, IEEE CS Press, Los Alamitos, Calif., 1998

[5] Hayton, R., Bacon, J. and Moody, K.: OASIS: Access Control in an Open, Distributed Environment. Proceedings IEEE Symposium on Security and Privacy. IEEE CS Press, Los Alamitos, Calif., 3–14, 1998

[6] Hine, J.H., Yao, W., Bacon, J. and Moody, K.: An Architecture for Distributed OASIS Services. Proceedings Middleware 2000, Lecture Notes in Computer Science, 1795. Springer-Verlag, Berlin, Heidelberg and New York, 107–123, 2000

[7] Lloyd, M.: Conversion of NHS Access Control Policy to Formal Logic. MPhil in Computer Speech and Language Processing, University of Cambridge, 2000

[8] Ma, C., and Bacon, J.: COBEA: A CORBA-based Event Architecture. In Proceedings of the 4th Conference on Object-Oriented Technologies and Systems (COOTS-98), USENIX Association, Berkeley, 117–132, April 1998

[9] W. Yao, K. Moody, J. Bacon. A Model of OASIS Role-Based Access Control and its Support for Active Security. In *Proceedings, Sixth ACM Symposium on Access Control Models and Technologies (SACMAT)*, Chantilly, VA, May 2001

[10] Synapses Project Deliverables, Trinity College, Dublin see http://www.cs.tcd.ie/synapses/public/html/projectdeliverables.html

[11] The Patients's Charter (for England), January 1997 see http://www.doh.gov.uk/pcharter/patientc.htm

[12] UK Government White Paper, "The New NHS: Modern, Dependable", December 1997, see http://www.doh.gov.uk/nnhsind.htm

[13] UK Government White Paper, "Information for Health", September 1998, see http://www.doh.gov.uk/nhsexipu/strategy/index.htm

[14] UK Government White Paper, "The NHS Plan - A Plan for Investment, A Plan for Reform", July 2000, see http://www.nhs.uk/nationalplan/