Access Control Policy Management

October 2000 - September 2003
support for a PhD student, Wei Wang, £56519

Grantholders: Ken Moody and Jean Bacon
km, jmb@cl.cam.ac.uk, http://www.cl.cam.ac.uk/Research/SRG/opera
University of Cambridge Computer Laboratory

1 Background and Overview

1.1 Project web pages

Please see *http://www.cl.cam.ac.uk/Research/SRG/opera/publications/* for annotated summaries of our publications on Policy Mangement, Business Contract Management and Access Control as well as the detailed citations of all the papers. Information on this and related projects can be found at: *http://www.cl.cam.ac.uk/Research/SRG/opera/projects/*

1.2 Background and motivation

This research arose from our work on RBAC (role-based access control) for distributed systems comprising multiple domains of loosely-coupled, heterogeneous services (OASIS: Open Architecture for Secure, Interworking Services). As the OASIS design and implementations progressed we became increasingly aware of policy issues that extended the work and were beyond the scope of the funded work: EPSRC GR/M75686, "OASIS Access Control: Implementation and Evaluation".

The origin of OASIS (Open Architecture for Secure Interworking Services) was in Richard Hayton's thesis in 1996 (EPSRC-funded). He started work on the principal-specific, capability-based access control designed for our Multi-Service Storage Architecture (MSSA) (EPSRC GR/H13666). He made the capabilities (signed certificates) role-based and extended their use to an open, heterogeneous service context. We presented the work at the ACM SIGOPS European workshop in 1996, at IEEE-ICDCS in 1997 and at IEEE-Oakland in 1998. EPSRC GR/M75686, "OASIS Access Control: Implementation and Evaluation" funded a PhD student, Walt Yao, to carry the research forward. One of the outputs of this grant was a formal model for OASIS, presented at the ACM SACMAT Conference in 2001. The paper was later extended for journal publication, see [5]. The project description and final report can be read at:
http://www.cl.cam.ac.uk/Research/SRG/opera/projects.

OASIS is an access control system for open, interworking services in a distributed environment modelled as domains of services. Services may be developed independently but service level agreements allow their secure interoperation.

OASIS is role based but has important differences from other RBAC schemes.

- Roles are service-specific; there is no notion of globally centralised administration of role naming and privilege management.
- Roles may be parametrised, as required by applications.
- Roles are activated within sessions. A session is started by activating an initial role such as *logged_in_user*, at which point strong authentication takes place. Roles may have activation conditions that require prerequisite roles, and a dependency tree of active roles is built up within a session.

- All privileges are associated with roles. We use appointment instead of privilege delegation; the activation conditions of roles may include appointment certificates. Persistent credentials (as opposed to session-limited role membership certificates (RMCs)) are implemented as appointment certificates.

- We provide an *active security environment*. Constraints on the context can be checked during role activation; the role may be deactivated if particular conditions become false subsequently.

Sandhu, in [14] provides a widely adopted model and our papers give details of related work. [3] gives a detailed comparison of OASIS and PERMIS.

The expression and enforcement of role activation and authorisation policy is a major component of the design and implementation of OASIS. Agreements between services in different administrative domains must be set up to support multi-domain interoperation. An example is a national Electronic Health Record (EHR) service comprising EHR services and many hospitals, clinics, primary care domains etc. Policies from national law and local administrative policies must be integrated and policies must be able to evolve. This grant enabled our research to be extended in these areas.

Our first candidate for the studentship was Andras Belokosztolszki. However, he was fortunate in obtaining a fully funded (for a Hungarian with overseas fees) PhD scholarship and has carried out his PhD research in the area of the grant. We were therefore able to offer the studentship to another PhD applicant Wei Wang, from the Edinburgh Masters course. David Eyers, a mature PhD student who started in October 2001 and is supervised by Dr Moody, has continued the OASIS research and has worked closely with Andras and Wei.

2 Design and implementation details

The research carried out during the project has been directed towards its original goals, but the actual technologies adopted have been somewhat different from those proposed.

Soon after the proposal was submitted the company marketing the POET ODMG compliant ODBMS changed its academic pricing structure, and we were quoted EUR 20,000 in August 2000. Instead we went for the public domain object-relational DBMS PostgreSQL [11], which Andras Belokosztolszki knows well. Andras extended its trigger mechanism to support a fine resolution active predicate store, with a flexible registration interface. Clients can request to be notified of any change to tuples that match a template; the range of templates supported is expressive. This piece of work was presented to the database group at Birkbeck College in January 2002. The foils are available on the Web [6]. We are confident that the PostgreSQL data model is appropriate and sufficient for our purposes. It is also suitable for use in applications, since it supports almost all SQL constructs, and has interfaces for binding object data structures into its object-relational tables.

The period of the grant saw sudden growth in the popularity of XML, and the rapid deployment of tools of every kind for managing XML data. In 2002 an industrial strength implementation of OASIS was developed above J2EE in connection with an EHR demonstrator. This project used the policy syntax and semantics described in [5], storing specific policies in an XML format. Our initial work on this grant took place above that implementation, though we have since developed two distinct research prototypes. In the interests of portability we have adopted this XML policy representation, suitably extended to meet any specific needs that have arisen in our research.

The main thrust of the proposed research was to investigate access control policy management for distributed applications. This work has been successfully pursued by the three PhD students named above. Among the highlights of what has been achieved are the following:

Policy components: We have extended the OASIS RBAC model in order to support the long-term evolution of policies. By naming every component in a policy we enable descriptions external to a policy specification to refer to individual policy components, which is essential for fine-grained

management; we have also defined privileges for managing policy at this fine grain, including *bind* and *unbind* primitives that guarantee the semantic integrity of policy components during update.

Meta-policies: We have separated organisational policies into parts that directly relate to access control decisions and those that encode the general goals of access control within the organisation. We can use this classification to coordinate policy evolution and distributed policy management.

Compliance policies: These express fine-grained restrictions and requirements for policies. Compliance policies are invariants to which successive policy versions must adhere. They have their own component model, and are well-suited to describing the fundamental properties of an interworking group of policies. In this way administrators can maintain organisational goals as policy evolves.

Interface policies: These significantly reduce the problems of scale associated with change during collaboration between domains that each manage their own policy. Service level agreements can be established on the basis of conformance with an interface policy; the cooperating domains can then make changes independently, provided that their policies still conform to the specified interfaces.

This work was presented at the Policy 2002 conference [8].

Contexts: We have introduced contexts, a construct that allows us to structure policy components from multiple aspects. Contexts introduce an indirection between the entities that manage policies and the policies themselves, allowing managers to refer to related policy parts independently of their version, naming, and implementation. We have used contexts for a number of purposes, among them controlling information flow during policy enforcement. The idea has been extended to hierarchical contexts, which offer the possibility of scalable policy management, if necessary up to Internet level.

Access control to policies: We have introduced a set of privileges that enable OASIS RBAC policies to treat stored RBAC policies as resources and to control access to them. These privileges allow fine-grained policy update to take place securely. They may also use contexts to ensure that policy managers only carry out modifications that lie within their competence.

This work was presented at the Policy 2003 conference [10].

The thrust of this research has been to investigate how long-term policy evolution can be supported by meta-policies and privileges for policy management. Andras Belokosztolszki has for his PhD developed one of the two prototype RBAC systems mentioned above. Desert provides a set of interfaces and their implementation for the policy components that we have introduced, and offers a practical means to experiment with policies structured in that way, and to check their conformance to meta-policies. It supports visualisation tools that help to manage policy evolution. Also, through the privileges described above, Desert supports fine-grained access control for policy modification, which is vital for the management of a policy store.

Contrary to what was suggested in the proposal, this approach does not depend on having active database storage. We validate policy changes through appropriate interfaces at application level. Policy management is an essentially synchronous process if carried out in this way. This approach will not however scale well for truly global applications, for which asynchronous notification of policy modification will be required.

Our current thoughts on policy storage, including the use of active database technology, were presented at the WETICE-2003 conference [9]. Wei hopes to complete his PhD before the end of the present academic year, focussing on aspects of active database support for policy management.

3 Research output and follow-on research

Dr Moody gave a keynote on policy management for an NHS EHR application [12].
Initial work on an approach to expressing policy at a higher level than XML (for the computer non-specialist) was presented at the first international workshop on Policy for Distributed systems and networks Policy01 [4].
The three graduate students have published papers with us in the area of the grant [8, 9, 10].

We presented a paper comparing OASIS RBAC with PERMIS, which was developed at Salford as part of an EU project [3]; the comparison included aspects of policy expression.
Dr Bacon has two other PhD students working in related areas. Alan Abrahams has worked on contract-based application control [1, 2] and Brian Shand on the integration of policy with resource management and accounting [15].

We have given seminars at IBM Almaden (US) and Hursley (UK), Agilent Edinburgh, Hong Kong University, Glasgow Caledonian University, Victoria University, Wellington NZ, Technical University of Darmstadt Germany, University of Birmingham, University of Hull, Birkbeck and Queen Mary Colleges London, at the 1999 NHS workshop in Cambridge, to the NHS Security group in Birmingham, at several subsequent NHS meetings, and at a BCS meeting in Coventry.

4 Related and ongoing work

David Eyers has developed the second research prototype extension to OASIS RBAC in connection with work towards his own PhD. This is our first fully active implementation; his distributed RBAC system (EDSAC21), which includes a Prolog inference engine, has been integrated with the Hermes publish/subscribe infrastructure [13]. Hermes communication depends on an overlay network built using secure tunnels. See [7] for a description of our recent work in developing secure publish/subscribe messaging systems.

David is at present implementing support for Dynamic Separation of Duties within EDSAC21; his implementation uses contexts, and depends on the publish/subscribe infrastructure. Another possible use of contexts is the association of roles belonging to particular context elements with various stages of a business process. Such a use of contexts can help workflow specifications in which workflow is partly enforced through the information flow restrictions between context labels.

At present we do not have a first-class active database within EDSAC21, but Wei and Andras are upgrading the t5 system to take advantage of recent PostgreSQL support for PL/SQL; we are also modifying the client registration and notification interfaces to use Hermes publish/subscribe.

One immediate application of this support will be to monitor active security conditions that depend on data managed externally. OASIS RBAC allows active environmental predicates (*memberships conditions*) that are held in a database to be a prerequisite for role activation. Applications will now be able to maintain data in a standard PostgreSQL database, and include database content among the active security criteria.

One of the main motivations for our research is to develop a distributed store that can be managed by many policy administrators in a controlled way. We have contributed much to the consistent evolution of such policies, but there are many issues remaining that need to be addressed. For example, consistency monitoring depends on synchronous checks that are initiated through the management interface. This is acceptable for a small or medium-sized enterprise, but it will not scale well for an organisation such as the NHS, for which asynchronous techniques are essential. The use of a well-engineered SQL DBMS extended by a fine-grain active predicate store should bring a number of advantages. Among them are support for distributed transactions in order to enable safe concurrent policy management, and the potential to trigger consistency checks asynchronously.

5 Resources

The resources were used as requested. Wei Wang has been supported to carry out a PhD in the research area of the grant. We have used the travel and subsistence support £6000 to attend some of the named conferences, to make national and international visits and to give seminars.

6 Summary

The objectives were ambitious for what was a modest grant (one PhD student). They were fully achieved and additional research was carried out, since several PhD students were attracted to work in the area.

References

[1] A. S. Abrahams and J. M. Bacon, Representing and Enforcing E-Commerce Contracts Using Occurrences Proc 4th International Conference on Electronic Commerce Research (ICECR4), pp.59–82, Dallas, Texas, USA, November 2001

[2] A. S. Abrahams. Developing and Executing Electronic Commerce Applications With Occurrences PhD Thesis. University of Cambridge Computer Laboratory. September 2002

[3] J. Bacon, K. Moody, D. W. Chadwick and O. Otenko. Persistent versus dynamic role membership In 17th IFIP WG3 annual working conference on Data and Application Security, Colorado, August 2003

[4] J. Bacon, M. Lloyd, and K. Moody. Translating role-based access control policy within context. In *Policy 2001, Workshop on Policies for Distributed Systems and Networks*, Bristol, UK, Springer LNCS 1995, pp.107–119, 2001

[5] J. Bacon, K. Moody, and W. Yao. A model of OASIS role-based access control and its support for active security. *ACM Transactions on Information and System Security (TISSEC)*, 5(4):492–540, November 2002.

[6] A. Belokosztolszki. The t5 predicate store. Seminar given at Birkbeck College in January 2002, see http://www.cl.cam.ac.uk/∼km/Active_DB-AB.pdf.

[7] András Belokosztolszki, David M. Eyers, Peter R. Pietzuch, Jean Bacon, and Ken Moody. Role-based access control for publish/subscribe middleware architectures. In H.-A. Jacobsen, editor, *2nd International Workshop on Distributed Event-Based Systems (DEBS03)*, ACM, June 2003.

[8] A. Belokosztolszki and K. Moody. Meta-policies for distributed role-based access control systems. Proceedings of the Third International Workshop on Policies for Distributed Systems and Networks (Policy 2002), Monterey, CA, USA, pp.106-115, June 2002

[9] A. Belokosztolszki, D. Eyers, W. Wang and K. Moody. Policy Storage for Role-Based Access Control Systems. WETICE-2003, Enterprise Security, Linz, Austria, 2003.

[10] A. Belokosztolszki, D. Eyers and K. Moody. Policy Contexts: Controlling Information Flow in Parameterised RBAC Policy 2003: IEEE 4th International Workshop on Policies for Distributed Systems and Networks, Lake Como, Italy, pp.99–110, June 2003.

[11] B. Monjian. PostgreSQL: Introduction and Concepts Addison Wesley, 2000

[12] K. Moody Coordinating policy for federated applications In 14th IFIP WG3 annual working conference on Data and Application Security, Schoorl, Netherlands, August 2000, Proceedings Kluwer pp.127–134, 2001

[13] Peter R. Pietzuch and Jean M. Bacon. Hermes: A Distributed Event-Based Middleware Architecture. Proceedings of the 1st International Workshop on Distributed Event-Based Systems (DEBS'02), July 2002.

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

[15] B. Shand and J. Bacon. Policies in Accountable Contracts. Policy 2002: IEEE 3rd International Workshop on Policies for Distributed Systems and Network s, Monterey, California, U.S.A., pp.80-91, June 2002.