Editorial

Role Based Access Control – A Solution with its own Challenges

As businesses, government agencies, and individuals commit ever-growing volumes of information to computer systems, and as networks (and ultimately, Grids) provide increasing levels of connectivity between these systems, there is a concomitant need to ensure that this information can only be accessed or modified by those who are authorised to do so. Equally, there is a need to ensure that such authorisation does not exceed what is necessary for the purpose in hand, and that it respects the wishes of those who may provide, or be the subject of, the information.

When dealing with a comparatively straightforward aspect such as personal finance, a data subject will want an individual member of a domain institution such as a bank to have access to their current data when dealing with a new transaction, without necessarily wanting their full financial history of ten years earlier in a different town to be revealed. Similarly when it comes to health data, in the data subject's (patient's) opinion it may be highly desirable to restrict individual health professionals' access to current episodes, replicating the physical restriction inevitable with paper records, although this may not always match what is desirable, or indeed wished for, by the patient once circumstances change. The classic cited example of the ideal is when a person has an emergency health episode whilst on holiday and can be admitted without prior notice to the nearest hospital, which can then gain real-time access to the patient's main health records wherever they are located. But the obverse has less appeal – patients (and indeed health professionals) cannot countenance the reciprocal scenario, whereby any health professional can access any aspect of a patient's record in any location with regard to any part of their previous history.

Protection of confidentiality on computer systems has usually been addressed through processes that are concerned with *authenticating* a user's identity and *authorising* access to information on the basis of their role(s), privileges, or attributes. For individual resources, a process of *access control* through permissions is then used to recognise when an authorised user may read or modify information. While generally tractable for individual systems, this model is less suited to a distributed context, much less so to one where the information is distributed across autonomous and independent agencies, as occurs increasingly in many businesses, and overwhelmingly in healthcare, a domain that forms the main exemplar for this special section. It also assumes a static context, whereas, during the working day an individual may undertake many roles, which could well have quite different responsibilities.

In these circumstances, both in health care and in other domains, role based access control (RBAC) would appear to offer the ideal solution. Its form reflects the established management structures that incorporate a number of easily defined levels of access. Indeed, hospitals are probably the most common domain for the use of RBAC, although it has also been used in the National Security Agency (NSA) and US Inland Revenue Service. It ensures that access to information is restricted according to the function an individual professional or operative is undertaking, thereby enabling them to know as much as they need to know, but no more, for their current role.

However, on closer inspection, the picture is still somewhat blurred, even for healthcare. Some of the challenges posed by the need to interpret the concept of *role* are (briefly) outlined below:

- *Professional role.* It would appear at first sight to be comparatively easy to differentiate the roles of doctors, nurses, other health professionals, and support staff in the same way that a

bank clerk authorising a withdrawal needs less information than a mortgage adviser authorising a long-term loan. However, not least in the health sector, even this is not that simple. On the one hand, each of the principal health professions would submit that professional sub-divisions are important for role based access – for instance a gynaecologist being regarded as different from an orthopaedic consultant, or a psychiatric nurse from general nurse. But conversely roles are also blurring, with nurse practitioners now having some prescribing powers, while a health visitor will have a considerable interest in a mother's past history of depression.

- *Organisational role.* Almost all healthcare and other services are delivered by organisations. Persons only operate within those organisations to undertake a particular role within their professional group. Thus there is an attraction in linking record access to their organisational function – the receptionist will have access to information about appointments in a specific department, the doctor to recent and past diagnostic and consultation outcomes, and so on. As many healthcare organisations such as hospitals are large with a significant number of staff, this approach also enables a further reduction in access – for instance the nurse on a surgical ward having access only to current episode aspects of a patient's record, largely different to the aspects to which a psychiatric nurse needs access. This can also enable access to be restricted to the records of particular groups of patients, such as the patients on the ward on which the nurse is working. The problem with this approach is that it assumes a largely static workforce, whereas in the real world a person may be redeployed at short notice to cover unplanned staff absence. Clearly, it would not be appropriate for a nurse redeployed urgently from general surgery to paediatrics not to be able to have access to the records of the children on that ward to which s/he was temporarily allocated, especially when this is in the face of a short-term crisis, so that s/he has no prior knowledge of the individual cases. Thus, systems of access based on organisational role can only be effective if they are also linked in some way to highly dynamic and effective yet secure systems for updating attributes arising from organisational roles, whether temporarily or permanently.
- *Teams.* Teamwork would also appear a necessary aspect to considering possibilities for defining role and duty of care; and it too provides challenges. Increasingly, healthcare is delivered by functional teams – whether they be established teams on the surgical ward or *ad hoc* virtual teams in primary care or child protection. Role based access could be hypothesised for the team treating the patient, possibly with some sub-division along professional lines as well. But teams are not static; they are dynamic in two ways. First, with the natural pattern of staff progression team members go and others come, and thus role based permissions must be constantly changed. Secondly, and more challenging still, teams may be extended on the basis of a particular patient's need. Thus a psychologist may be drawn into a community mental health team to support the treatment of one particular patient. The school nurse may be drawn in to the primary care team supporting a child from a disadvantaged family. These extensions may be quite short term or fluid, so that in effect individual patients each have a personalised "virtual team" [1].

There is much more that could be discussed about roles (including the role of the patient [2]), but for our purposes, the above should be sufficient to indicate that while RBAC offers a way forward — like most technological solutions, it also poses some challenges of its own.

Our own interest in this area arose from our collaboration as members of the IBHIS project (Integration Broker for Heterogeneous Information Sources) funded by the U.K.'s Engineering & Physical Sciences Research Council (EPSRC). This project aimed to explore the use of software service architectures for drawing information together from distributed, heterogeneous information sources in order to provide information to a clinician, and the necessary models and the demonstration prototype of IBHIS were developed by a team of software engineers from the

universities of Durham, Keele and UMIST, together with Keele's *Centre for Health Planning & Management* [3,4].

This focus upon the use of distributed autonomous information sources means that the operations of the broker need to comply with a complex set of access control needs. So, to ensure that the access control model developed for IBHIS was rigorously assessed, and took full account of current research, the IBHIS project sponsored a workshop on RBAC in January 2004, drawing together research expertise across the United Kingdom. The short experience paper, and the three full papers, that are presented in this special section are expanded versions of the main presentations from that workshop. They are largely, but not exclusively, centred upon the needs of the healthcare domain and indeed, it is important to recognise that RBAC has much wider application. For example, web content management systems are now used widely in academia and business to manage information that may need to be updated and accessed by a whole range of individuals with different responsibilities. The first paper is therefore a useful reminder of this wider generality of the use of RBAC.

The short experience paper by Marshall describes how the challenges provided by the needs of academic course administration — which has many characteristics that parallel those of healthcare — have been addressed through two projects, TOBIAS (Tools for Object Based Integrated Administration of Systems) and NESS (Newcastle E-learning Support System). Both of these treat roles as being *filters* between the user and the resources, but implement the concept in very different ways. A key conclusion from this paper is that while roles are *necessary* in such a context, they are unlikely to be *sufficient*, as illustrated by the examples provided.

The paper by Longstaff *et al.* bridges between the general use of RBAC for complex web applications and its role in healthcare. The authors describe the use of their well-established Tees Confidentiality Model (TCM) for providing access control within an RBAC context, involving processing a range of *permission types* that can be used to permit or deny access to a given resources. A particular strength of the approach that they have adopted is that it makes it possible for a clinician to over-ride access restrictions in a structured manner when emergency situations arise.

An RBAC architecture that has been designed specifically for use with Electronic Health Records (EHRs), and that is based upon the established and more general OASIS (Open Architecture for Secure Interworking Services) model of RBAC, is discussed in the paper by Eyers *et al.* The solution adopted for integration of EHRs depends upon the existence of some 'common keys' (which will occur in the context of the U.K.'s National Health Service (NHS) context) and retains a human element for the task of joining record fragments from different sites. The paper reviews the benefits and limitations of such an approach and illustrates it by discussing the form and behaviour of their prototype system.

Finally, the paper by Turner *et al.* examines how these models have been adapted and extended within the context of the more general-purpose IBHIS broker discussed above. A particular challenge for IBHIS is the potential autonomy of the data sources (and hence the corresponding lack of any ready means of indexing between them). Within IBHIS this is addressed chiefly by creating a Data Access Service (DAS) as a service 'interface' for each data source (a similar 'wrapper' mechanism is employed in OASIS), together with semantic matching based upon a common ontology. The resulting 'hybrid' S-DAC model (Service-enabled Data Access Control) seeks to employ key features from existing models, an in particular, to extend these to support data access by teams.

This set of papers inevitably focuses largely on one small area of application — although healthcare is undeniably a very important one, and it is also one that is a particularly rich source of examples and challenges — as these papers demonstrate! Equally, they describe a range of approaches to meeting the needs of RBAC within this context, each with its particular strengths and limitations. Together, we believe they represent a valuable summary of current research in this important area, and one that is both valuable for the healthcare domain as well as also potentially of much wider significance. It is also a significant presage of the growing importance of this topic that the workshop was held just as the RBAC model from NIST (National Institute of Standards & Technology) was being adopted by ANSI [5].

The editors would like to thank the authors who so willingly extended their original workshop contributions for this special section, and in particular, the many anonymous referees whose work played an important part in putting this section together and ensuring that it is representative of best current practice and knowledge.

Keith Bennett
Michael Rigby
David Budgen

References

[1] Rigby M, Roberts R, Williams J, Clarke J, Savill A. Lervy B, Mooney G. (1998. Integrated Record Keeping as an Essential Aspect of a Primary Care Led Service; British Medical Journal, 317, 579-582.

[2] Rigby M. (2004). Information as the Patient's Advocate; in Rigby M (ed.) Vision and Value in Health Information; Radcliffe Medical Press, Oxford, 57-67.

[3] Turner, M, Zhu, F, Kotsiopoulos, I, Russell, M, Budgen, D, Bennett, K, Brereton, P, Keane, J, Layzell, P, and Rigby, M. (2004). Using Web Service Technologies to create an Information Broker: An Experience Report, in *Proceedings of ICSE 2004*, IEEE Computer Society Press, 552-561.

[4] Budgen D, Turner M, Kotsiopoulos I, Zhu F, Russell M, Rigby M, Bennett K, Brereton P, Keane J and Layzell P (2004). Managing healthcare information: the role of the broker. in *Proceedings of Healthgrid 2005*, Oxford, April 2005, IOS Press, 3-16.

[5] http://csrc.nist.gov/rbac/