A GENERAL MODEL OF AUTHORISATION FOR COMPLEX COMPUTING APPLICATIONS

Jim Longstaff, Mike Lockyer, Tony Howitt, Ian Elcoate, Paul Massey
School of ComputingUniversity of Teesside, Middlesbrough TS1 3BA, England

Keywords: Access Contol, Authorisation Models.

Abstract: We present the principles of permissions processing used in the Tees Confidentiality Model (TCM), a general authorisation model which is suitable for complex web applications in addition to computer systems administration. In particular, we present new techniques for authorising by multiple concepts, and also for overriding access restrictions. A database implementation of the TCM is referred to, which can be used to provide the basis for a general authorisation service. The TCM is an extension of Role-Based Access Control (RBAC), and has had a significant impact on the development of healthcare computing in the UK. A demanding scenario from Electronic Health Records is used to illustrate the permissions processing and the power of the model.

1 INTRODUCTION

An authorisation model, through its implementation within an identity and access management system, provides facilities to enable users, whether they be human end-users or other computer systems, to use resources in specified ways. This can range from using sophisticated application facilities to the simple querying of data.

Identity and access management systems are usually perceived as consisting of three parts: authentication, for establishing the identity of the user; authorisation, for determining the resources that the user is permitted to use; and administration. One application for these systems is to provide access control for distributed web-based applications. The Tees Confidentiality Model (TCM) is a powerful model for authorisation, and is unique in that it includes override capabilities (Longstaff, 2003a), (Longstaff, 2003b), (Longstaff, 2002). The TCM lends itself to implementation by database systems, and we discuss elements of its implementation by Microsoft Transact SQL.

The following sections show how the TCM can be used to model and implement the kind of authorisations debated for the national Electronic Health Record (EHR) development for England, called the Care Records Service (CRS) (Gaunt, 2005), (NPfIT, 2003), (NPfIT, 2005). We focus on permissions processing by order of complexity, defined according to the number of concepts in a permission type. We have been advised that there are many applications in eGovernment and eCommerce that could benefit from the TCM functionality.

We start by outlining a scenario which demonstrates the need for powerful authorisation functionality in healthcare. We assume all interactions with EHRs will be auditable.

2 HEALTHCARE SCENARIO

2.1 Patient-specified 'Sealed Envelope' Authorisations

This part of the scenario was written by a Consultant Transplant Surgeon. It concerns a fictitious patient who we will refer to as Alice, and her GP, who we will call Fred. Alice is 50; some of the major events in Alice's medical history are summarized as follows

- She had a pregnancy termination when she was 16
- Was diagnosed diabetic at 25

Longstaff J., Lockyer M., Howitt T. and Elcoate I. (2005).
A GENERAL MODEL OF AUTHORISATION FOR COMPLEX COMPUTING APPLICATIONS.
In *Proceedings of the Second International Conference on e-Business and Telecommunication Networks*, pages 74-79
DOI: 10.5220/0001421200740079

- End Stage renal failure when she was 45
- Renal transplant at 48
- Acutely psychotic at 49
- Crush fracture of T12 aged 50

Let us now suppose, not unreasonably, that Alice expresses the desire to place the following confidentiality restrictions on the availability of her medical records data about two of these conditions (i.e. she wishes to place them in a patient's Sealed Envelope, in CRS terminology):

1. My GP, Fred, can see all my data.
2. Nobody must know about my termination except my GP, any Gynaecological Consultant, and the Consultant Renal Transplant Surgeon who operated on me.
3. My GP, Consultant Renal Transplant Surgeon and Consultant Orthopaedic Surgeon can see my psychosis data, but no-one else.

Let us add the following contrived requirement (but still one which a health records authorisation system must be capable of implementing):

4. I do not wish the members of the hospital team who carried out my termination operation to be ***ever*** able to see my psychosis data, except if they are viewing in a psychiatric role.

In one of our TCM demonstrators, these confidentiality requirements can be specified using electronic consent forms (Longstaff, 2002).

2.2 Health Service Authorisations

Let us also consider the authorisations that Health Care Practitioners (HCPs) will be entitled to access data based on their role, and a 'Legitimate Relationship' with the patient, generally meaning that the patient is registered with them, or has been referred to them.
The following extracts from the CRS requirements specification - the ICRS OBS (NPfIT,2003) - illustrate the complexity of the proposed authorisation functionality.

730.20.2 *A user has a Legitimate Relationship with a patient if they are currently involved in providing care to the patient, or are a member of a health and Social Care team which is providing care to the patient. For example, a practice nurse in the same team as the patient's GP would have a Legitimate Relationship with the patient. If a GP wished to exclude the nurse from inheriting the Legitimate Relationship, the nurse would be excluded from the defined team. In support of this, it must be possible to establish Legitimate Relationships with workgroups as well as individual users.*

730.16.2 *Health information systems must be capable of granting access to records based on workgroups.*

2.3 Override Capabilities

We must add to these requirements that they must be capable of being overridden in carefully controlled and auditable ways. Override for the CRS system has been described as 'breaking the seal" on a Sealed Envelope. Our original scenario included the following requirement.
Suppose Alice has been scheduled for a transplant. Tests lead the surgeon to suspect a previous pregnancy (if the tissue type of the father is similar to the graft a very serious rejection may ensue). However Alice refuses to confirm a previous pregnancy. The surgeon then elects to use an override facility (Specific Override, as described below, section 5.2), which enables him to discover and view the termination data. A safe treatment can then be planned.
A further type of override, based on the concept of Collection, is described below in section 5.4 .

3 A TCM APPLICATION FOR HEALTHCARE

We now proceed to demonstrate how the access restrictions described in the scenario can be handled by a single mechanism, which forms part of the TCM. To do this, we must firstly introduce some basic TCM concepts.

3.1 Collections

A *collection* has *elements*, which may be *members* or other collections. Collections and elements are uniquely-identified. Collections are inherently hierarchical in that they can contain sub-collections, which in turn can have their own sub-collections. Elements can participate in more than one collection. *Confidentiality permissions* (see below) are defined with inheritance properties in collections.

Collections are used for all structuring purposes in the TCM, e.g. forming identities into teams, and positioning roles into role hierarchies. A discussion of collections, and the use of permissions for collections, is given in section 5.3 below.
The preferred TCM mechanism for confidentiality permission assignment is based on the concept of collection. However, it is possible to assign confidentiality permissions to Roles using general and limited role hierarchies in the established RBAC ways (Ferraiolo, 2001), (ANSI-INCITS), 2005).

3.2 TCM Applications Design

We introduce the following TCM concepts by indicating their role in application development.
The development of a TCM application involves the following steps:

- Establishing *identities* (users), and *protected objects* (objects accessed and used).

  For the EHR projects, the identities are Health Care Practitioners (HCPs, e.g. doctors, nurses), and patients. The protected objects are patients' EHRs, with authorisations specified to the granularity of their constituent parts (which we call EHRobjects).

- Determining the *identifiers* for both identities and protected objects.

  Patients in the UK are identified by NHS Number; HCPs by various national and local registration codes. Identifiers for EHRobjects are determined by the designers of EHR software.

- Specifying ***authorisation classifiers (***or ***classifiers)***, which are criteria to be used in authorisation.

  Authorisations are specified and enforced for members of collections conforming to classifiers, by confidentiality permissions. Names for classifiers are chosen by the application designer.

  The classifiers associated with identities we will call *Identity*, *Role*, and *LegRel*, and for protected objects *EHRobjectID*, *EHRobjectType*.

- Defining the practically useful *confidentiality permission types (CPTs)*, generated from the full range of previously-specified classifiers (see below for details)

- Choosing the required *overrides* from the full range generated from the previously-specified confidentiality permission types (see below).

It is also possible to have classifiers for *operations* on protected objects, but here we just consider a single operation classifier corresponding to the read operation.

3.3 Confidentiality Permissions

Classifiers are used to specify confidentiality permission types (CPTs), which must contain at least one Identity Classifier, one Operation Classifier, and one Protected Object Classifier.
We will now describe an example of a CPT, and its corresponding instances, which we call ***confidentiality permissions*** (CPs). (Note that we present an informal description, which assumes downward inheritance for classifier collections.) The notation we use for this CPT is as follows:

CPT2 (IdentityID, LegRel || R || EHRobjectID)

A CP which is an instance of the CPT2 type specifies a read authorisation involving an Identity Collection (e.g. a clinical team, workgroup or just a single identity), for which a Legitimate Relationship exists with the patient, and an EHRobjectCollection (e.g. psychosis data for this patient, including any subcollections such as medication prescribed for psychosis). It therefore grants or denies access to identities having Legitimate Relationships to specific collections of data.
CPs are processed in order of precedence according to complexity (ie the number of classifiers present in the CPT specification). If two CPTs exist with the same number of classifiers, then the CPT with a higher precedence classifier (as specified by the applications designer) is processed first.

Now we are able to suggest a TCM for healthcare. From the range of all possible CPTs, the following ***might*** be selected as being practically useful as a base set for the CRS. ***(Note that a final set of permissions would only be arrived at following a detailed TCM design exercise, which is to be***

funded by the NHS National Programme for Information Technology). They are listed in the precedence order in which they are processed.

CPT1 (IdentityID,Role, LegRel ||R||EHRobjectID)
CPT2 (IdentityID, LegRel || R || EHRobjectID)
CPT3 (Role,LegRel || R || EHRobjectID)
CPT4 (Role,LegRel || R || EHRobjectType)

Note that we only consider and explain read permissions; the TCM generally allows for multiple operation classifiers to be defined.

4 PERMISSIONS PROCESSING FOR HEALTHCARE

We now illustrate how the Confidentiality Permission Types listed in the previous section may be used to represent the constraints on data access described in the healthcare scenario.

Query by Fred, for termination data

Suppose that Fred queries Alice's Electronic Health Record (EHR), with authorisations controlled by the TCM. He will see the data for the termination, because the permissions would be processed in the following order:

- CPT1: IdentityID, Role, LegRel || R || EHRobjectID (none, for Fred)
  (no match)
- CPT2: IdentityID, LegRel || R || EHRobjectID (read, for Fred)
  match, data displayed
- CPT3: Role, LegRel || R || EHRobjectID (denial)
  (ignored)
- CPT4: Role, LegRel || R || EHRobjectType (inherited read)
  (ignored)

The CPs are searched by order of type, i.e. CPT1, CPT2, … CPT4, to find the first CP with classifer values which match this user (Fred) and protected object (Termination Data). The first permission to be found is a CPT2 permission. This causes the data to be displayed. The search algorithm stops, which means that all remaining permissions are ignored, or overridden by search order precedence. (In our current demonstrator, this is implemented entirely as database searching, programmed in Transact-SQL).

Query by a GP other than Fred, for termination data

- CPT1: IdentityID, Role, LegRel || R || EHRobjectID (none for this GP)
  (no match)
- CPT2: IdentityID, LegRel || R || EHRobjectID (none for this GP)
  (no match)
- CPT3: Role, LegRel || R || EHRobjectID (inherited denial, for GPs)
  match, data not displayed
- CPT4: Role, LegRel || R || EHRobjectType (inherited read, for GPs)
  (ignored)

The first permission to be found for this user and data is a CPT3 permission, which denies access to the user acting in this role, even though he has a legitimate relationship with the patient.

5 OVERRIDES FOR HEALTHCARE

A identity would generally need to be authorised to use an override, and would have to subsequently justify its use. Electronic notifications would be sent to appropriate authorities when an override is used.

5.1 Override Types

There are four types of basic override defined for the TCM EHR application.

- *Specific override*, a CPT override which cancels any negative (denial) effects of CPT1-CPT3 permissions, leaving CPT4 and operating. This will enable the enquirer to see the information he would normally see by virtue of his role, and any specialist Work Area authorisation.
- *Team override*, a Classifier Collection override (see section 5.3), which enables an Identity to view data read-authorised to a higher-level of Identity Collection
- *Role Override*, a Classifier Collection override, which enables an Identity to view

data according to the Confidentiality Permissions granted to a higher-level Role Collection.
- *Global Override*, which removes all restrictions on data.

5.2 Overriding Alice's requirements by HCP

In the Specific Override example described in section 2.3, the permissions processing for the termination data, for the Transplant Surgeon is as follows:

Transplant Surgeon with Specific override, for Termination data

- CPT1: IdentityID, Role, LegRel || R || EHRobjectID (none for this TS) *(SpecificOverride)*
- CPT2: IdentityID, LegRel || R || EHRobjectID (none for this TS) *(SpecificOverride)*
- CPT3: Role, LegRel || R || EHRobjectID (inherited denial, for TS role) *(SpecificOverride)*
- CPT4: Role, LegRel || R || EHRobjectType (inherited read, for TS role) ***Match, data displayed***

A CPT4 permission has now provided read access for the TS role, the denial by the CPT3 permission having been cancelled by Specific Override.

5.3 Overriding within Collections

We now give an example of overriding within Identity Collections. In order to do this, we firstly discuss the concept of Identity Collection and its associated permission processing.

Generally speaking, collections associated with Identities, and containing identifiers for Identities, can be used to model naturally-occurring team/subteam, or committee structures. The assignment of Identities to Identity Collections would mostly be made on the basis of Role – e.g. an anaesthetist is needed at a certain level in a team. Teams may have a temporary existence (being formed for a single task), and may exist in a succession of versions (members being replaced, for whatever reason).

Consider a simple abstract team (identity collection) structure shown in Figure 1. Here we have a Team T1, with its members M11, M12 (perhaps senior members, team leaders). It also has subteams, T11 and T111, which in turn have junior members M111, M1111, etc. An example of a team might be a Surgeon's team, formed for the purpose of carrying out emergency operations during a fixed time period; subteams could include an Anaesthetist Team, administration teams, and also teams of Theatre Nurses and Ward Nurses.
Suppose the situation arises that selective sharing of data between members of the team is required: members of T1 and T11 need to have access to data which is not to be usually made available to T111: this can be achieved by the assignment of confidentiality permissions as shown.

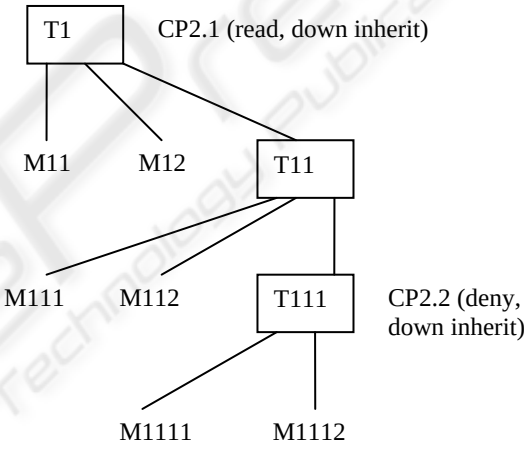

Figure 1: Team/subteam, with permissions, for a specified EHRobjectCollection

Consider an emergency situation where a junior member of a team, say M1111, needs to have access to the clinical data which has been made available to more senior members. (M1111 might be the secretary for the Anaesthetist Team, who has just received an emergency telephone call). Suppose that M1111 has been granted the privilege of using Team Override to the level of T11, and she elects to do so. She will now be able to access the data, because T11 and its members inherit the access assigned to this data at level T1.

6 CONCLUSIONS

We have illustrated the TCM authorisation model with examples from electronic health records. The TCM has previously influenced the ICRS OBS (NPfIT, 2003) (the requirements specification for the EHR for England) and has been implemented by several suppliers to the NHS as part of the ERDIP Programme. It is currently being used as part of a major project to further model and design the information governance model adopted by the National Health Service in England (based at the University of Teesside and funded by the UK Government). It also forms part of a new location privacy project, supported by industry, concerning the monitoring and tracking of individuals and items. Additionally, it is also being evaluated and applied within a location privacy project at the University of Minnesota.

REFERENCES

Longstaff JJ, 2003a. Longstaff JJ, Lockyer MA, Nicholas J. The Tees Confidentiality Model: an authorisation model for identities and roles, ACM SACMAT 2003, Como, Italy, ACM ISBN 1-58113-681-1.

Longstaff JJ, 2003b. Longstaff JJ, Lockyer MA, Nicholas J. An Authorisation Model for complex web applications, ISSE 2003 Conference and Procedings, www.eema.org/isse.

Longstaff JJ, 2002. Longstaff JJ, Thick MG, Capper G, Lockyer MA. Eliciting and recording eHR/ePR Patient Consent in the context of the Tees Confidentiality Model, HC2002 Conference, Harrogate, England.

Gaunt N, 2005. UK NHS Care Records Guarantee http://www.e-health-insider.com/tc_domainsBin/Document_Library0282//nhscr_guaranteev1.pdf

NPfIT, 2003. Integrated Care Records Service, Output Based Specification. National Programme for IT, England, http://www.dh.gov.uk/assetRoot/04/05/50/52/04055052.pdf

NPfIT, 2005. National Programme for IT, 2005, www.npfit.nhs.uk

Ferraiolo DF, 2001. Ferraiolo D F, Sandhu R, Gavrila S, Kuhn D R, Chandramouli R (2001) “Proposed NIST Standard for Role-Based Acess Control”, ACM TISSEC, Vol 4, No 3.

ANSI INCITS. 2004. ANSI INCITS 359-2004, American National Standard for Information Technology: Role Based Access Control www.incits.org