Use Case – Syllabus Plus Web Room Booking system

Scenario
Throughout the University there are approximately 350 rooms, made up of teaching rooms, laboratories and conference spaces. A system has been put in place by the Timetable Services team, to manage the scheduling of bookings for these rooms; they are timetabled using the Scientia Syllabus Course Planner. A web based booking system is made available for University staff to book the rooms, however there are a few rooms which are only bookable by either Timetable services or the room owner.

95% of the rooms throughout the campus are bookable by all members of staff, whilst the remainder do have restrictions on who can book them, for example the specialist rooms such as laboratories are only available to be booked by a select number of staff. Control over who can book particular rooms must be exercised based upon an individual’s position and role within the organisation, in effect requiring a form of role based access control.

Syllabus plus provides an Authorisation manager to enable this role based control, yet it is not deemed suitable by the project team for the administration of these roles. This is due to the authorisation manager not having in place structured data which would allow for the delegation of access control based upon a member of staff’s position within the University.

The Grouper group management tool is designed to allow for the structuring of such organisational data. On a nightly basis Newcastle University’s organisational data is loaded into Grouper, with this data we are able to create a tree like representation of the University’s organisational hierarchy. Each team throughout the University is represented within Grouper as a source group. It also provides a number of roll up groups, which are made up all source groups which live under a particular departmental branch. For example all teams that live under the ISS branch, would be represented within an ISS All role up group.

The use of Grouper combined with the Syllabus Plus system has been selected as the best way forward to provide the access control required for this scenario. The structure and the granularity of this delegation can be approached from a number of angles. The following will discuss the forms of delegation required and also discuss the possible approaches for provisioning the access control.

Actors/Components
- All University staff members
- Timetable services
- Room Owner
- Grouper
- Syllabus plus System

Form of Delegation
The key areas of delegation are required;
- Controlling who can book the rooms throughout the University
- Control by team membership – access dependant on which team staff are a member of i.e. ISS-Middleware team.
- Control by departmental membership – access dependant on a departmental branch i.e. ISS-All.
- Specialist rooms – in some cases it is not appropriate to allow all members of a team/department to be able to book a room. The specialist rooms such as the laboratories can only be booked by a select group of people. It should therefore allow individual members of staff to be giving access to book a room.

- Schools and services manage internal spaces and room bookings
  - Allow the delegation of management for room bookings to be assigned to a service team or school.
- Control of the roles
  - A form of delegation is also required for the management of the roles. It will need to control who is able to assign users to the different roles.

**Approaches and Considerations**
A scenario on this scale does result in a number of possible approaches to the structuring and implementation of the required access control. These approaches need to take into consideration a number of different factors including scalability, manageability and also usability.

In this scenario one of the key areas to consider is how important it is to limit a user’s ability to book a room based upon their place in the organisation. As discussed in the scenario, for certain rooms, such as the laboratories this is a key factor, it would not be appropriate to allow all departments to book specialist rooms such as these. On the reverse to this, there are rooms which are not deemed as specialist rooms, conference rooms are a prime example of this, would it be necessary to only allow individuals members of teams to book these rooms.

**Access Control on a Room Basis**
A logical approach to a solution for this use case would be to provision access control on a room by room basis. As figure 1 shows within Grouper it would be possible to represent all rooms throughout the campus as a group and then delegate access to these rooms by assigning memberships. The room structure would be loaded on an automated basis, making use of the corporate data made available through one of the outputs of the IDMAP’s project, the [Institutional Data Feed Service](#), resulting in an accurate representation of the rooms available for booking.
Figure 1: Proposed structure for delegation on a room by room basis

This can be combined with another data structure which is represented within Grouper, Newcastle University’s Organisational hierarchy (Figure 2). The system administrator can make use of this structure to delegate access control to teams/departments throughout the University, whilst still having the capability of assigning access on an individual basis.

This approach will allow for access control to be delegated on varying levels from a very restrictive fine grained approach to a more flexible high level approach. The fine grained approach, of assigning individuals to rooms, would be used when controlling access to the specialist rooms. Whilst the less fine grained approach will be used to assign access on a departmental basis to those rooms which are not deemed as specialist rooms.

This would meet the criteria in terms of the delegation that is required for this use case, yet there a number of key issues that need carefully considered for this approach. The first of which is the number of rooms that would be required to be loaded into Grouper, approximately 350 rooms would need to be represented as groups within Grouper. This is achievable from a technical perspective, yet it is the administrative perspective which would cause concerns over its feasibility as an optimal approach.

As each room would represent a role, it would create an administrative burden for the system administrator, who would be responsible for maintaining the memberships for each of these roles. Although many of the memberships will be made up of source groups from the Organisational Structure there is still a responsibility by the system administrator to monitor the access lists.

Overall this approach does offer a very fine grained approach to the delegation of access control, as each room would have its own specific list of staff members and teams who would be able to book...
it. Yet, as a consequence of this finely grained approach it does lead to a resultant administrative burden upon the system administrator.

As the room booking system will already have all room data loaded in, this approach also means that you are creating the room structure in both Grouper and in the application. This is another part of the overall process maintenance which could be avoided with other approaches.

Grouper will be used as the source of data for user information in the new system, such as login details, department information; it will also of course provision the user’s access groups. With the structure as discussed above, users could be assigned to a large amount of user access groups, which would all need to be loaded into the new system. The amount of data that is being provisioned between Grouper and the new room booking system is a key factor that would need careful consideration. Loading 350 access roles along with potentially thousands of memberships per role could potentially lead to server performance issues. Limiting the amount of data that is moving between the two systems would be a more sensible approach, and this could be avoided with the second approach.

![Organisational Hierarchy in Grouper](image)

**Figure 2: Organisational Hierarchy in Grouper**

**Role Based Access Control**

It is often the case that certain groups of rooms that are located within the same buildings will inherit the same set of pre-requisites to be satisfied before allowing members of staff to book them. For example two rooms maybe booked by only two members of staff, Bob and Sally, whilst the other two rooms are bookable by the whole of the computing department. In the above approach, this
would be dealt with by having four separate access groups for each room, and would be structured as shown in figure 3.

![Diagram](image_url)

**Figure 3: Possible room booking structure**

Effectively this means in this example that you have two sets of two groups which are made up of exactly the same memberships, which in turn requires four times the amount of administration. This is just a small subset of rooms, and the amount of rooms which would have the same membership lists would be on a much larger scale. A logical approach to overcome this would be to implement a role based approach.

As part of the new room booking system, the Syllabus Plus authorisation manager allows for role based access control to be applied. All room data is of course loaded into the system, it is then possible to group these rooms together depending on their room type. As an example it could group all general ISS meeting rooms within Claremont Tower into an “ISS-General Meeting Rooms” group. It could then group all the ISS-Specialist rooms together into an “ISS-Specialist” group. In effect each of these role groups would then have an individual access list of users who are able to book the rooms which are contained in this role group.

These role groups could then be created within Grouper, as shown in Figure 4, which would manage the delegation of access, by making use of the Organisational Structure. This would mean that there would be no need to create groups for each of the 350 rooms within the University campus, and as a result lowers the amount of administration required. Instead the system administrator would only need to maintain and manage memberships for the newly created role groups.
Figure 4: Role Based Access control

They will be able to make use of the departmental source and all groups from the Org structure, to delegate access on a member of staff’s position within the University. This could be used to delegate access to the more general role groups, such as the “ISS-General” group. The ISS_All group could be added as a member to this group which would allow all members of ISS to be able to book any rooms which are assigned to this role in the room booking system. It will also be possible to assign individuals to the access groups for the more specialist roles.

There is also an element of inheritance within this approach, take the Kings Gate roles for example, anyone who is a member of the Kings Gate Gen 1 or 2 group automatically should also be able to book any rooms related to Kings Gate Gen. So by adding the Gen 1 and 2 roles to the Kings Gate Gen role, means that any users within these roles will automatically be able to book any room under the general tag. This removes the need to add these users to two separate role groups, reducing the amount of administration that is required.

This approach still allows for a fine grained level of delegation with the advantage of a reduced administrative burden. The system administrator is still able to restrict access down to an individual level as per the first approach, but by assigning them to a role group they do not have to duplicate the effort each time a new user requires booking rights to a specialist room.

Syllabus Plus and Grouper
As discussed in both approaches above, Grouper and Syllabus Plus play an important role in the delivery of access control to the web room booking system. Figure 5 shows the processes and interactions involved between Grouper and Syllabus Plus if the second approach was adopted. This diagram also represents the processes for the delivery of the first approach, although the mapping of roles would of course differ. The diagram shows that Grouper is responsible for the delegation of
access control whilst Syllabus Plus is responsible for the mapping of roles to the room sets and delivering the end user authorisation for room bookings. Syllabus Plus delivers the control over which rooms a member of staff can book, yet it is Grouper that delegates the access control. By making use of Grouper to provision the access control rather than the Syllabus Plus authorisation manager, system administrators are able to use the loaded organisational data to delegate access control on a departmental basis.

With both approaches, it will be necessary to export the role groups and membership details from Grouper and feed this data into the Syllabus Plus Authorisation Manager database. Syllabus Plus provides an import tool which parses an XML file to import user data and roles, which allows for data to be easily ported across from Grouper into the system.

As the delegation of access control is done within Grouper, if a user was added to a role, Syllabus Plus would not be aware of this change. It would be possible to set the data feed between the two systems to be as near to real time as possible, however each time a data load is required, the full data set is required to be loaded in, which would not be feasible to do on a regular interval. After consideration a nightly update to the roles has been agreed, the project team agreeing that the ability of new users being able to access the system instantly is not a key factor.

**Initial Conclusions**

Both approaches have the possibility to provide a sensible level of delegation for access control, yet both approaches differ when it comes to the administrative perspective. The first approach does have a large amount of administration involved to maintain the access lists for each of the rooms. If the relevant admin was carried out on these room access groups it would ensure that only the exact set of people would be able to book the room. The second approach does take a slightly higher level approach, by grouping users into the different role groups. There are some assumptions involved in this approach, by assuming that if a member of staff can book one specialist room they can book any other specialist rooms within a building. These are all factors which need to be balanced when deciding upon the best approach to satisfy this use case.
Figure 5: Interactions between Grouper and Syllabus Plus

The above diagram shows the main processes involved in porting Grouper groups in Syllabus plus. Roles are created within Grouper to match those that have been created in Syllabus plus, staff members are then assigned to these roles making use of the corporate data that has been fed in. A nightly export of these roles and memberships is scheduled, which combines this data with a corporate data feed which provides information such as a user’s department, position, to produce an XML file which can be imported into the Syllabus plus system. Within the Authorisation manager the defined roles are mapped to the different room sets which a particular role is able to book. The imported memberships are then mapped to the different roles which then allows the web room booking to determine which rooms a user can book.