Access Control

Goal

The purpose of this laboratory exercise is twofold: to provide hands on experience with the specification and enforcement of authorization policies and to provide an experimental framework for discussing access control policies. Students are assumed to have completed the Authentication lab.

Access Control Scenario

Consider the printserver scenario defined in the Authentication lab. The print server supports the following operations:

> `print(String filename, String printer);` // prints file *filename* on the specified *printer*
> `queue(String printer);` // lists the print queue on the user's display in lines of the form *<job number> <file name>*
> `topQueue(String printer, int job);` // moves *job* to the top of the queue
> `start();` // starts the print server
> `stop();` // stops the print server
> `restart();` // stops the print server, clears the print queue and starts the print server again
> `status(String printer);` // prints status of printer on the user's display
> `readConfig(String parameter);` // prints the value of the *parameter* on the user's display
> `setConfig(String parameter, String value);` // sets the *parameter* to *value*

Not everybody working in the company has the same rights to access the print server. Alice is managing the print server, so she has the rights to perform *all* operations. Bob is the janitor who doubles as service technician, he has the rights to *start, stop* and *restart* the print server as well as inspect and modify the service parameters, i.e., invoke the *status, readConfig* and *setConfig* operations. Cecilia is a power user, who is allowed to *print* files and manage the print queue, i.e., use *queue* and *topQueue* as well as *restart* the print server when everything seems to be stuck. Finally, David, Erica, Fred and George are ordinary users who are only allowed to *print* files and display the print *queue*.

Lab Work

The first task is to modify the prototype print server developed in the Authentication lab, so that it implements the necessary code to enforce the access control policy outlined above. This means that all registered users must be included in the password-file/-database defined in the Authentication lab. This first implementation should be based on an access control list for the print server, i.e. the print server is considered as a single object with the different methods as the possible operations. The access control list must be specified in an external policy file, or another form of external media, that is loaded when the print server starts, i.e. the policy *must not* be hardcoded into the program.

The second task is to identify roles and define a role hierarchy and permissions for each role, so that the access control policy outlined above can be implemented. The third task is to develop a second prototype, based on the prototype developed in the authentication lab, which enforces the access control policy using Role Based Access Control, i.e. based on the role hierarchy and permissions defined in Task 2. The role hierarchy must be specified in one or more external policy files, or the same form of external media used in Task 1, that is/are loaded when the print server starts.

Now consider the situation where Bob leaves the company and George takes over the responsibilities as service technician. At the same time, two new employees are hired: Henry, who should be granted the privileges of an ordinary user, and Ida who is a power user and should be given the same privileges as Cecilia.

The final task is to implement the necessary changes in the access control policy specifications of the two prototypes developed in this lab, so that they reflect the organisational changes in the company. The experience gained from these modifications will allow you to compare the management support for the two policy enforcement mechanisms, i.e. the flexibility and facility with which organisational changes can be reflected in the access control policy. This comparison must highlight the strengths and weaknesses of each implementation and discuss the expressive power and the ease of management supported by the two policy specification abstractions, e.g., which organisational changes are easily captured in both implementations and which are more easily specified in one implementation than in the other.

Evaluation

This lab is a mandatory part of the course, which means that you have to hand in a small report, which will be evaluated and counts toward your final grade. The report should follow the normal structure of a report, and we recommend that you use the following structure:

1. **Introduction** (max 1 page)
   The introduction should provide a general introduction to the problem of access control in client/server applications. It should define the scope of the answer, i.e. explicitly state what problems are considered, and outline the proposed solution. Finally, it should clearly state which of the identified goals are met by the developed software.
2. **Access Control Lists** (max 2 pages)
   This section should provide a short overview of the implementation of the access control lists and the motivation behind all non-trivial design choices.
3. **Role Based Access Control** (max 3 pages including diagrams)
   This section should document the results of the *role mining* process performed in in Task 2 and provide a short overview of the implementation of the role based access control mechanism implemented in Task 3 along with the motivation behind all non-trivial design choices. In particular, it must describe the syntax used to specify the RBAC policy.
4. **Evaluation** (max 4 pages)
   This section should document that the prototype enforces the access control policies defined in this assignment; both ACL and RBAC and both before and after the changes.
   The evaluation should provide a simple summary of which of the requirements are satisfied and which are not.
5. **Discussion** (max 2 page)
   This section documents the reflections and discussions of the final task.
6. **Conclusion** (max 1 page)
   The conclusions should summarize the problems addressed in the report and clearly identify which of the requirements are satisfied and which are not (a summary of Section 4). The conclusions may also include a brief outline of future work.

The laboratory work will be assessed in the same way as the other reports on the course (i.e., you are welcome to hand in the report in groups). The full report should be limited to a maximum of 13 pages, excluding the source code. Source code for this lab should be included in a separate zip-archive.

Although the maximum limit for the report length is 13 pages, it is expected that most reports will be shorter.

The report and source code should be handed in electronically, on DTU Learn, before 23.59 on Friday 25 November.

Useful Links

- Role Based Access Control

Christian Damsgaard Jensen Christian.Jensen@imm.dtu.dk
Last modified 5 November 2022.