

Delegation and Authorisation Management for Middlewares

A Proposal for a Pilot Project using Rotor

Babak Sadighi and Erik Rissanen

Swedish Institute of Computer Science (SICS)
Policy Based Reasoning Group
babak,mirty@sics.se

Background and Objectives

In a project called "Authorisation MANAGEMENT for Distributed Applications" (AMANDA) funded by Microsoft Research in Cambridge, UK, we have developed a framework and a Calculus of Privileges [FSB01,FS02] for decentralised management of privileges such as access permissions. The main idea is to move focus from "Who is permitted to perform an action" to "Who has the authority to create a permission or to delegate an authority". The notion of *constrained delegation* was presented in [BDF02], that gives a general formalisation of delegation chains. In this way it is possible to decentralise, for instance administrative duties, while still maintaining a centralised control over the system as a whole.

We have now developed an authorisation server, called *Delegent*, partially based on the results of the AMANDA project. We have successfully used the server in prototype applications, and it is currently under further development. An application may update and query the authorisation repository, thus supporting an easy implementation of complex authorisations in a generic way.

However, there is a trend to more complex and capable middleware systems, and we wish to consider what kind of authorisation services the middleware layer services might need, and what role our delegation model could have. The .NET framework represents a modern platform for middleware architecture, so it would serve as a suitable setting for our purposes.

The Common Language Infrastructure (CLI) has a model for permissions and a stack walk to determine that a component is authorised for a specific permission. In order to make the middleware components "authorisation aware" in the *Delegent* sense, we need to translate the *Delegent* permission model to the CLI model. In this way it would be necessary to make the CLI execution environment call *Delegent* to determine what permissions should be allowed when a component requests a permission.

With this project we aim to fund our initial steps to study needs, possibilities, and benefits of our delegation model in a middleware architecture.

Interesting research issues are:

- At what level should delegation and authorisation services be placed in the system architecture? What benefits or drawbacks would there be with the

run-time environment enforcing the access control compared to having the applications responsible for it?

- Would applications be easier to develop, less buggy and more effective if the middleware services, that the applications use, would be "authorisation aware"?
- How easily can we make the run-time environment call *Delegent*?
- Does the CLI environment put any specific requirements or constraints on our delegation model?

Participants

Babak Sadighi

Babak Sadighi is a researcher at Swedish Institute of Computer Science (SICS) and the principal investigator of the Policy Based Reasoning Group at SICS (www.sics.se/isl/pbr). Sadighi was the project leader of the AMANDA project funded by Microsoft Research. He is currently managing a R&D project for an authorisation component in a military command and control system in collaboration with Swedish Defence Material Administration and SAABTech systems.

Erik Rissanen

Erik Rissanen has a MSc. degree in Software Engineering with computer security specialisation from Royal Institute of Technology. Since October 2001, Rissanen is working in the Policy Based Reasoning Group and his main responsibility is the development of *Delegent*.

Deliverables

As the deliverable of this project we will produce a report and a short paper based on our studies to clarify in what circumstances and how our delegation model is useful for authorisation services in middlewares and in particular in .NET infrastructure. Moreover we will examine what are the necessary extensions for *Delegent* to be used in the CLI environment.

References

- [BDF02] Olav Bandmann, Mads Dam, and B. Sadighi Firozabadi. Constrained Delegations. To be published in Proceeding of IEEE Symposium on Security and Privacy, May 2002.
- [FS02] B. Sadighi Firozabadi and M. Sergot. Revocation Schemes for Delegated Authorities. To be published in Proceeding of 2002 IEEE Workshop on Policies for Distributed Systems and Networks, June 2002.
- [FSB01] B. Sadighi Firozabadi, M. Sergot, and O. Bandmann. Using Authority Certificates to Create Management Structures. To be published in Proceeding of Security Protocols, 9th International Workshop, Cambridge, UK, April 2001.