

WORKSHOP 8

Distributed access control

Author: Bo Öhrström (Danish National Library Authority, Copenhagen, Denmark)

Introduction

The opening of the Internet for broad public use has in the nineties started an explosion of information. Everybody could begin to publish information for free use produced with tools, which became increasingly more simple and intuitive. The retrieval of information has in general been handled by search machines, which during the last decade have been developed to perfection in speed and efficiency. These search machines can find information placed on directly accessible web pages, while information in deeper database structures is handled by special interfaces with search capabilities.

The possibilities for doing business on the Internet or just protect information from free access created a demand for access management systems and methods. In the library world the prime example of new business became the publishers deliveries of electronic full text journals and databases. These products were placed directly on the Internet, and the publishers only managed access to the information by simple control of the IP-number of the user's PC. Normally an institution like an university bought unlimited access to a product for all its researchers and students, and the access would be controlled by the publisher by opening for access from all known IP-numbers of the university.

During the years the number of products and services with managed access has risen, and the users are expecting access to these from any location at any time of the day. The complexity of giving the correct user the access to the right mix of products and services is increasing.

Distributed access control

Access control or access management is governed by the three As:

- Authentication
- Authorisation
- Accounting

Authentication is the task of making sure, who the user is, while authorisation is the activity of deciding, what the user is allowed to do based on the user's identity and other sources of information. Accounting is procedures connected with the registration of the user's amount of usage of the resource. In the following only authentication and authorisation is discussed.

Access control can be centralised or distributed, and for the sake of simplicity the two solutions could be defined in this way:

Workshop Discussion Papers

Centralised access control: One central system, which is able to both authenticate and authorise users. The following access to the access controlled resource is directed through the central system (by a proxy) or directly to the resource (for example based on a time-limited ticket).

Distributed access control: More distributed systems, which are able to authenticate and/or authorise users. The following access to the access controlled resource is directed through more proxies or directly to the resource (for example based on a time-limited ticket).

An associated demand for a user is simultaneous or near simultaneous use of several resources and services. In this case necessary authentication and authorisation should only happen once seen from the user. In other words the function called single sign-on is of high priority.

Authentication can be based on several methods. Usernames and passwords are a very common, and the use of digital certificates is emerging. In the first case usernames and passwords should not be transmitted in clear text to avoid theft of these. In the latter case security are high, but complexity in maintaining the system and lack of standards is challenging the use. Finally it will always be an evaluation of the risk of the possible losses, that will determine the level of security and the complexity of the authentication solution.

Authorisation is typically not tied closely with an individual but more often to groups of users. After authentication normally the user is given the rights of a specific user group to access a selection of electronic resources.

Today several solutions have been created to handle authentication and authorisation, and more systems are under way. Well-known systems in the academic area are the Athens system (UK) and the Shibboleth project (USA).

Questions to guide discussion

A. Status and experiences

What are the status and experiences in the different countries regarding the presence and usage of access control systems?

B. Existing solutions Athens, Shibboleth...

Which systems are on the market or will be available soon. What are the pros and cons, and which are considered usable seen from the different countries ?

C. Central or distributed, large and small institutions

What are the architectural and organisational trends and what are the pros and cons for both?

Workshop Discussion Papers

D. Authentication and certificates

How usable are certificates in the authentication process ?

E. Authorisation and granularity

Which level of granularity is requested for authorisation and how centralised should the authorisation process be?

F. One identity for each service or one identity to all services

Single Sign On - how important is it for the user to carry the user identity in a seamless way between services?

H. Recommendations

Which recommendations can be given for future work and activities in the area of "Distributed access control" - and what will be the future?

Related links:

Athens - <http://www.athensams.net/> and
<http://www.athensams.net/development/athensssoandda.html>

Shibboleth - <http://shibboleth.internet2.edu/>