Information Use–Control in E–Government Applications

Antonio Maña
University of Málaga, Spain

Mariemma Yagüe
University of Málaga, Spain

Stamatis Karnouskos
Fraunhofer Institute FOKUS, Germany

Habtamu Abie
Norwegian Computing Centre, Norway

INTRODUCTION

Within the process of globalization and the permeation of all areas of life by technology, electronic government (e-government) is becoming a powerful tool that will effectively integrate and manage the huge amount of existing information, as well as seamlessly integrating citizen interaction with its services (Abie et al., 2004). E-government is the use of ICTs in public administration in combination with organizational changes and the development of new skills, in order to improve public services and democratic processes, and to strengthen support for public policies. The concept of mobile government (m-government) refers to the use of mobile wireless communication technology within government administration and in its delivery of services and information to citizens and firms (Ostberg, 2003). Digital government is a general term which includes e-government and m-government. In this digital world the management and protection of digital information content, and the rights associated with this, from unauthorized access, use, and dissemination has been a matter of concern for many rights holders. Moreover, the protection of privacy has been a matter of great concern for many citizens.

BACKGROUND

Access Control In Digital Government Scenarios

When security requirements for digital government applications are considered, authorization often emerges as a central element in the design of the whole security system. Many other security requirements depend on the flexibility, trustworthiness and expressiveness of the authorization scheme. Authorization in conjunction with access control, which is the mechanism that allows resource owners to define, manage and enforce the access conditions that apply to each resource (Reuters, 2001) form the key concepts in the core of digital rights management (DRM).

Among the traditional access control models, role-vased access control (RBAC) is commonly accepted as the most appropriate paradigm for the implementation of access control in complex scenarios. RBAC can be considered a mature and flexible technology. Numerous authors have discussed its properties and have presented different languages and systems that apply this paradigm.

However, very dynamic environments with a high volume of heterogeneous data, like semi-structured data systems, DRM repositories, digital libraries, Web services, digital government systems, and so forth require more flexible constructions for the expression of access control policies. In RBAC, the structure of groups is defined by the security administrator and is usually static. The grouping of users is not flexible enough to cope with the requirements of more dynamic systems where the structure of groups cannot be anticipated by the administrators of the access control system. However, this is exactly the case in digital government applications, and especially with the secure interoperability between different governmental agencies. In such a complex heterogeneous infrastructure, the integration of new resources and the application of fine-grained dynamic policies on them is of key importance. Traditional access control schemes cannot be applied as they are usually designed for use with static infrastructures and do not scale well.

Current access control models are not appropriate for DRM and other open, heterogeneous, and dynamic scenarios because access control is often erroneously considered to apply to locations" instead of objects or resources. Because of this, it is assumed that one or a few access control (enforcement) points are used to restrict access to a set of resources in one location.

In summary, we can conclude that a different approach is required in order to solve the scalability problems of these systems, to facilitate dynamic fine-grained access control management and to provide the means to express access conditions in a natural and flexible way. Furthermore, access control models must take into account the fact that the creation and maintenance of access control policies is a difficult and error-prone activity.

The semantic access control (SAC) model (Yagüe et al., 2003a) provides an appropriate solution to the aforementioned problems, especially for heterogeneous, distributed and large environments such as digital government. As we will show later, the flexibility of the SAC model allows it to easily simulate other models such as mandatory access control (MAC), discretionary access control (DAC) or RBAC.

Digital Rights Management Technologies

The slogan "information wants to be free" was one of the reasons why in the early days the Internet was seen as a vehicle for the free floating of ideas and information. However, in the last few years this has drastically changed since many companies have realized the Internet's capabilities and its potential as a vehicle for marketing and selling goods and services. The copyright owners of these products therefore promoted the concept of DRM. DRM is an integrated complex context covering not only technologies that limit or prohibit the unauthorized copying or distribution of these products but also includes laws, contracts and licenses that regulate and restrict the use of such material (Becker, Buhse, Günnewig, & Rump, 2003).

Rights management applies to a wide variety of systems and objects, and because of this, it is almost impossible to consider all potential application scenarios. The approach must, therefore, be developed in an open and extensible way. Reuters has proposed the development of a taxonomy of Rights and Obligations for products and services (Reuters, 2001). We think that, even in the case where this taxonomy could be built in a sufficiently complete way, its applicability in the real world might prove challenging, mainly because rights and obligations can have different interpretations in different scenarios, countries, and so forth. Therefore, we propose an open approach, based on the explicit expression of the semantics of these rights and obligations. This approach allows users to better tailor the system to their needs and their particular context.

Usually, the content industries regard DRM as dealing with the problem of unauthorized downloading of copyrighted material, a practice that costs content creators and distributors dearly in lost revenue. However, an important and often overlooked fact is that DRM is closely related to the general field of access control. Therefore, rights enforcement involves an access decision about a resource subject to intellectual property rights.

From the technology point of view DRM technologies can control resource access (number, duration, etc.), altering, sharing, copying, printing, and saving via software or hardware implementations. In the majority of the DRM approaches today not only is anonymity prevented, but the privacy of the user is in danger, since often DRM systems facilitate the profiling of users' preferences which can lead to the identification of the consumer's real identity. DRM technology in the aforementioned context is a relatively new research field that has been rapidly developing since the mid 90s, whose results are controversial (Felten, 2003). DRM solutions have been developed by several companies, but most of them are proprietary in nature. Ongoing work in academia and industry promises exciting developments in the short and midterm. However, as yet, an established, widely accepted, open DRM system for the wired or mobile world does not exist.

The amount of information produced and maintained by governmental organizations is immense and traditional mechanisms can not efficiently cope with it. That, in conjunction with the efforts to come closer to citizens and interact with them on a 24-hour basis via Internet or mobile channels, is leading us to the adoption of new models and technologies in digital government. One such promising technology is DRM, and the need for an integrated DRM framework in digital government is real. DRM is used to control and meter the huge amount of digital information generated and disseminated. In digital government DRM can be used in its classical form as well as the other way round (i.e., providing privacy rights management (PRM) for citizens).

Classical DRM Usage in Digital Government

In its classical form DRM systems in digital government can protect governmental assets from unauthorized dissemination and enforce fine-grained policy models in connection with those assets.