Medical Informatics Europe 2002
G Surján et al. (eds)
IOS Press 2002

Access Control Administration in Healthcare Applications

MATTAS K. Andreas, MAVRIDIS K. Ioannis and PANGALOS I. George

Informatics Laboratory, Computers Division, Faculty of Technology,
Aristotle University of Thessaloniki, 54006, Thessaloniki, Greece.

Abstract. The interconnection of information systems of different parties involved in healthcare applications leads to the need for information sharing across large-scale and highly distributed database systems. Applying appropriate access control policies in an effective and flexible way is a specific task for a number of local security officers that must operate according to a high-level access control administration system. The particular security requirements of healthcare information systems are reflected to the access control system, which must be flexible and dynamically adaptable to the daily activities. Decentralizing access control administration can be achieved in a uniform and consistent way when applying appropriate administrative rules and constraints. In this paper are presented the basic features of an access control administration model for interconnected information systems, as in the healthcare environment.

1. Introduction

Healthcare information systems (HIS) are increasingly adopting today information technologies (IT) for electronic storage, transfer and processing of information. Furthermore, the implementation of specific applications in the healthcare sector (e.g. the Electronic Health Care Record) often demands the use of distributed and interconnected systems that spread over organizational boundaries. A major issue concerning modern healthcare institutions is their increasing interest in sharing access of their information resources in an internetworked environment. Security is an important issue in health care environments (HCEs) where large amounts of highly sensitive personal data are processed ([1], [5]). Healthcare information systems often need to support special requirements for the protection of personal and medical patient data.

In healthcare information systems, medical and logistics information is usually saved in database systems. A security policy for access control in medical database systems is thus needed in order to preserve the availability, integrity and confidentiality of the overall system ([7], [8]). A number of access control approaches has already been proposed in this direction ([2], [4]). However, as stated in [10], one of the main omissions in access control models is the authorization of the administration of access control systems. Access control is basically simple as long as the permissions do not change. This however scarcely happens in healthcare applications where information sharing is usually very dynamic ([2]).

In this paper, the administrative issues of traditional and modern access control approaches are discussed, as well as the advantages provided by the so-called active security systems that are especially useful in HCEs. Then, the basic features of a flexible administrative system for access control in dynamic and highly distributed healthcare information systems are introduced.

2. Access Control Requirements in Healthcare Environments

The protection of sensitive medical and personal data stored in healthcare information systems from unauthorized exposure, illegal modification and system failure is a major concern. It is important to ensure for example that no patient's life is endangered due to information-system error or to illegal modification of medical information. According to a recent report, for example, more than 1000 accidental deaths have occurred due to computer system failures ([3]). Another equally important concern is the assurance of the patient's privacy by allowing access to the medical record (especially sensitive information) only to authorized users. As a result, healthcare information systems require the use of appropriate security policies ([6]).

There are three major categories of security policies that are commonly used in computer systems: the discretionary policies, the mandatory policies, and the role-based policies. However, as has been demonstrated ([7], [8]), both discretionary and mandatory features, when used separately, are not sufficient in health care environments. The emerging role-based approach provides a way of enhancing traditional discretionary and mandatory approaches. Another important aspect of access control mechanisms, which recently gets increasing attention research, has to do with their active or passive character. The majority of well-known security models are characterized as passive ones, in the sense that they are based on subject-object relations, which are implemented using access control matrices, as well as lattice-based access controls. These models cannot distinguish between permission assignment and activation. According to [14], the security issues for clinical workflows associated with patient care aim to provide very tight, just-in-time permissions. Hence only the appropriate clinical staff can get access to a patient's records and only when they are providing care for the patient without adding any significant administrative overhead. As a result, there is a need for access control models based on the emerging context associated with tasks and activities. This depends on the particular patient, the location where the activity takes place and the time when access requests are submitted.

3. Types of Access Control Administration

Access control administration can be performed in various ways depending on the specific access control model used. Traditional access control administration varies between centralized approaches in mandatory or multilevel systems to decentralized (owner based) ones in commercial discretionary systems. In either case, a number of limitations have a significant impact on the efficiency of administering access control systems. Hybrid administration is also another approach, which combines the centralized and the decentralized administration and is exercised for different information in each case [15]. For example in healthcare applications there is a distinction between treatment of medical and logistics data.

In distributed healthcare computing environments there may be multiple, independent and geographically spread entities (individuals, organizations, institutes, notaries etc.) with authority to control access to their local resources. Each of these parties is responsible for defining access rules for the protected resources and bring its own set of concerns. Therefore, access control systems might allow administrative authority for a specified subset of objects to be delegated by the central security administrator to local security officers. For example, authority to administer objects in a particular region can be granted to the regional security administrator. Control over the regional administrators can be centrally administered, but local security administrators must have considerable autonomy

within their regions. This process of delegation can be repeated within each region to set up sub regions and so on [13].

In general, decentralizing the process of access control administration without losing central control over broad policy is a challenging goal for system designers and architects ([11]). There is tension between the desire for scalability through decentralization and maintenance of tight control. A complete solution to this problem requires further research and faces significant theoretical problems ([9]).

4. The Proposed Approach

In our approach, administration of access control systems is not only related to the need for decentralized services. It also provides the necessary mechanisms to preserve the internal consistency and integrity of the access control policy that is in effect. In such a perspective the access control system is examined as a security information system, which is set to one level higher than the regular information system of the organization. Special users, called administrative users, gain administrative permissions to exercise particular administrative operations on selected administrative objects, which in turn are the components of the access control system, such as normal users, roles, teams etc.

The aim of the proposed approach is to develop an access control administration system for large-scale and highly distributed healthcare information systems, which also exploits the security characteristics of the underlying access control system.

4.1. The Underlying Access Control System

Patient's information is usually the main target of a group of doctors and nurses (users) who are qualified to play specific roles in order to provide efficiently their services and are supported by the IT infrastructure of the HCE. The access to sensitive personal and medical data must therefore be controlled by a dynamically adapted access control system, which is transparently provided to the users, in order to ensure that access to information and services is granted only to authorized persons, without requiring them to deal with complex security mechanisms.

A representative access control model for healthcare environments that meets the above requirements is the well-known Hybrid Access Control (HAC) model ([2]). It incorporates the advantages of broad, role-based permission assignment and administration across object types and yet provides the flexibility for fine-grained activation of permissions for individual users on individual object instances. HAC reveals a promising access control model based on RBAC ([12]), which is a new approach that provides the means to simplify access control management in large-scale information systems. It also incorporates TMAC ([14]), which covers the cases of teams that sum up a group of users in specific roles with the objective of completing a specific activity in a particular context. In HAC the team concept is further used as a grouping mechanism that associates users with contexts. Besides the association of permissions to roles and users to roles, contexts are also associated with teams.

In the HAC model, contextual information is related to the persons that are affected and their personal data objects that are critical for a specific activity. In addition other factors, such as location and time, may also be taken into consideration. Users participate also in teams with a common task to accomplish. Thus, the permissions of particular members of a team are enriched temporarily and then filtered according to the current context of their activities ([2]). HAC takes into account the dynamically changing (by low level administrators or biometric devices) context, which is associated with an ongoing activity

in providing access control and thus distinguishes the passive concept of permission assignment from the active concept of context-based permission activation.

An access control system based on the HAC model can provide fine-grained (adjusted to protected objects), tight (adjusted to need-to-know requirements of subjects) and just-in-time (only when needed) permission activation for protecting objects (e.g. medical data) from excessively exposures to even authorized parties. However, in order to enforce uniformly and consistently an access control policy in large-scale and distributed HISs without introducing overwhelming administrative overhead, there is a need for an appropriate access control administration system. Such a system could incorporate the advantages of the underlying access control system and enforce a number of rules to regulate administrative activities into a well-controlled context of operation.

4.2. Main Features of the Access Control Administration Model

Access control administration is a continuous and complicated task that has to be performed within different conditions. The proposed access control administration model is based on the components of the HAC model in order to take advantage of an active behaviour in administrative tasks. In this way, can be achieved efficient administration of access control in large computing environments, with significant flexibility in controlling access to security metadata during the runtime.

Two phases of the access control administration process is distinguished:

1. Access control design, which is carried out in an offline state (build time). The security administrative staff captures the healthcare organization's rules and policies to define, name and construct the static components of the access control system. For example, static components of the access control system based on the HAC model include objects, operations, permissions, roles, teams and their structure. In addition, a number of hierarchies are constructed to reflect abstractions of the above definitions and to represent classification levels for multilevel access control abilities. The design process is accomplished according to the rules and constraints defined in a specific secure design methodology, as the one defined in [6].
2. Access control managing, which is carried out in an online state (run time) and copes with any daily or emergency activity in the HCE. The access control managing is accomplished mainly by the healthcare administrative staff (head doctor, head nurse, logistics) of the particular HCE and involves binding values to specific dynamic components of the access control system (e.g. define contexts and associate them with teams), while the HIS is in operation. For example, in a medical surgery center, there is a need for an emergency operation; the head doctor can arrange a surgery team to handle this case. Although the head doctor can work in the clinic as a surgery doctor, he can also be the potential administrator for a specific field of operations; this means that he gets the right to administer accessing to clinical information of a patient during a specific incident.

In order to facilitate the supporting of dynamic administration of access control, besides the use of administrative permissions and roles, the mechanisms of administrative contexts and teams are introduced. Administrative context identifies the specific abilities of each member of an administrative team to manage the access control system in a particular administrative domain of the distributed healthcare information system. An administrative domain is thought to be a part of an organization where a unique administration policy is in effect.

The access control administration model includes a number of formally specified administrative functions and operational components, which can be combined into a set of functional specifications for further product development and system evaluation.

5. Conclusions and Future Work

Sharing access to information resources of healthcare information systems that spread over organizational boundaries is a major issue concerning many modern healthcare institutions. In addition, healthcare information systems are characterized by the need to support the protection of personal and medical patient data. Large-scale and highly distributed information systems introduce additional needs for applying appropriate access control policies in an effective and flexible way. Decentralizing access control administration can be achieved in a uniform and consistent way when applying appropriate administrative rules and constraints in the context of a well-defined access control administration model. The proposed approach to such an access control administration model exploits the mechanisms and components of the underlying HAC model in order to apply the active characteristics in the administrative process.

In our future work we intend to develop a set of functional specifications of the access control administration model for healthcare environments. In more detail, this research work will focus on the definition of a methodology for specifying administrative components and their abstractions, associating them with administrative functions and assigning them to administrative users.

References

[1] Furnell S.M., Pangalos G., Sanders P.W. and Warren M.J., (1993), 'A Generic Methodology for Health Care Data Security', Medical Informatics, 19(3).
[2] Georgiadis C, Mavridis I. and Pangalos G. (2000), 'Context and Role Based Hybrid Access Control for Collaborative Environments', Proc. of 8th Workshop on Secure IT Systems - NORDSEC2000, Iceland.
[3] Gritzalis D., (1997), 'A baseline security policy for distributed healthcare information systems', Computers & Security Vol. 16, No. 8, pp. 709-719.
[4] Mavridis I., Pangalos G. and Khair M., (1999), 'eMEDAC: Role-based Access Control Supporting Discretionary and Mandatory Features', Proc. of 13th IFIP WG 11.3 Working Conference on Database Security, Seattle, Washington, USA.
[5] Pangalos G., (1996), 'Secure medical databases', Proceedings IMIA security conference, Finland.
[6] Pangalos G., Khair M., (1996), 'Design of a secure medical database system', in IFIP/SEC'96, 12th international information security conference.
[7] Pangalos G., Gritzalis D., Khair M. and Bozios L., (1995), 'Improving the Security of Medical Database Systems, Information security - the next decade', J. Eloff and S. Von Solms editors, Chapman & Hall.
[8] Pangalos G., Khair M. and Bozios L., (1995), 'An Integrated Secure Design of a Medical Database System', MEDINFO'95, The 8th World Congress on Medical Informatics, Vancouver, Canada.
[9] Sandhu R. S. and Munawer Q., (2000), 'The ARBAC99 Model for Administration of Roles', 15th Annual Computer Security Applications Conference, Phoenix, Arizona, USA.
[10] Sandhu R. S., (2001), 'Future Directions in Role-Based Access Control Models', International Workshop MMM-ACNS 2001, St. Petersburg, Russia.
[11] Sandhu R., Bhamidipati V. and Munawer Q., (1999), 'The ARBAC97 Model for Role-Based Administration of Roles.' ACM Trans. on Info. And System Security, 2:1, Feb. 99, 105-135.
[12] Sandhu R., Edward Coyne, Hal Feinstein and Charles Youman, (1996), 'Role-Based Access Control Models', IEEE Computer, Volume 29, Number 2, Feb. 1996, pages 38-47.
[13] Sandhu R and Samarati P, (1997), 'Authentication, Access Control, and Intrusion Detection'. The Computer Science and Engineering Handbook.
[14] Thomas R., (1997), 'Team-Based Access Control: A Primitive for Applying Role-Based Access Controls in Collaborative Environments', Proc. of the 2nd ACM Workshop on Role-based Access Control, USA.
[15] NIST, (2001), 'Computer Security Handbook', http://security.isu.edu/isl/hk_acces.html; 11/2001.