How to break access control in a controlled manner

Ferreira A[1], Cruz-Correia R[1,2], Antunes L[3], Farinha P[2], Oliveira-Palhares E[2], Chadwick D W[4], Costa-Pereira A[1,2]

[1]*Centre for Research in Health Information Systems and Technologies (CINTESIS), Faculty of Medicine*

[2]*Biostatistics and Medical Informatics Department, Faculty of Medicine*

[3]*Computer Science Department, Faculty of Science & LIACC*

University of Porto, Portugal

[4]*Information Systems Security Group, Computing Laboratory*

University of Kent, Canterbury, England

amlaf@med.up.pt

Abstract

The Electronic Medical Record (EMR) integrates heterogeneous information within a Healthcare Institution stressing the need for security and access control. The Biostatistics and Medical Informatics Department from Porto Faculty of Medicine has recently implemented a Virtual EMR (VEMR) in order to integrate patient information and clinical reports within a university hospital. With more than 500 medical doctors using the system on a daily basis, an access control policy and model were implemented. However, the healthcare environment has unanticipated situations (i.e. emergency situations) where access to information is essential. Most traditional policies do not allow for overriding. A policy that allows for "Break-The-Glass (BTG)" was implemented in order to override access control whilst providing for non-repudiation mechanisms for its usage. The policy was easily integrated within the model confirming its modularity and the fact that user intervention in defining security procedures is crucial to its successful implementation and use.

1. Introduction

The integration of heterogeneous information scattered over different places is one of the main goals of Electronic Medical Records (EMR) [1]. This is why the EMR is becoming an essential source of information and a very important support tool for the healthcare professional. The distributed nature of the information stresses the need for security requirements to be taken very seriously [2].

One of these requirements, access control, is the baseline for information security [3] allowing users to interact and use resources of a system. In the case of healthcare, authorisation procedures cannot be organized at a user level anymore, but need to be tackled in a hybrid approach. A series of structured and formal policies, models and roles must be defined [4].

The Biostatistics and Medical Informatics Department from the Faculty of Medicine of the University of Porto has recently implemented a Virtual EMR (VEMR) in order to integrate patient information and clinical reports from departments scattered around a University Hospital, Hospital S. João in Porto, Portugal [5]. With more than 500 medical doctors using the system on a daily basis, a proper policy and access control model were required in order to manage and monitor accesses to the system [6].

For traditional access control models there is usually an assumption that access permissions are known in advance, but in a real environment unanticipated situations may occur and there may be the need to be flexible because it is impossible to predict all cases [7]. Since a patient's health is paramount, it is important to be able to override the access permissions when a patient's health is at risk.

In such cases as these, a *Break The Glass* (BTG) policy can be used in order to break or override the access controls in a controlled manner. This concept is not new, it has been studied and introduced in several domains [7] [8].

Not only does it relate to Healthcare [9] but also to other domains where access to information needs to be provided in certain emergency or specifically defined situations.

In the case study described in this paper, the concept of *Break the glass* is innovative because it is being implemented within a specific access control policy and model that are already in place, and the characteristics of BTG were defined by the healthcare professionals who are the end users of the system.

The BTG policy should allow a user to override the rules stated by the access control model and access what he requests, although he was not previously authorized to do it. But in so doing, other BTG rules come into play which may monitor, record or report the user's actions, thus making him responsible for his actions after the fact.

The main objective of this paper is to describe the design and initial implementation of a BTG policy in the VEMR system, integrated within the access control model already in use.

Further, it presents the issues involved and specific requirements in terms of organizational and human processes that are needed in order to enforce the BTG rules.

2. Access Control Model

In order to provide access in a controlled manner there is the need for a formal definition, at an organizational level, of access rights according to roles, tasks and other specificities of the Institution. This should be stated within an access control policy that expresses the procedures, processes and needs of an organization.

The rules of this access control policy were specified by the Security Commission within the Hospital, and are as follows:

User's roles, permissions and access levels

1. medical doctors must be able to access information about all the patients, except for more sensitive information (i.e. HIV or cancer results);
2. appointed medical doctors may have access to restricted and more sensitive information, such as in 1, (this is defined on a case-by-case basis);
3. medical doctors must be able to add notes and comments relating to the information they are accessing, and view each others' notes;
4. nurses must have read access to the EPR of the patients registered within their department;
5. healthcare researchers may have temporary access to the system for R&D purposes;
6. there is a different login that is restricted and used only for educational purposes (i.e. to learn how to use the system);
7. administrative staff have no access to the system at present;
8. only a few defined IT professionals have full access to the system to be in charge of its management.

Required mechanisms

a) all users of the system must be uniquely identified;

b) auditing and monitoring mechanisms have to be in place at all times, for all users;

c) administrative information about the users of the system has to be regularly updated;

d) *break-the-glass* mechanisms must be implemented so that people can access information for which they are not authorized to access (especially in cases of emergency or system error); users must be warned beforehand of what they are doing and a notification must be sent to his/her responsible superior.

The model implemented [6] (Figure 1) is hybrid in the way that it uses both Role-Based Access Control (RBAC) [10] and Identity-Based Access Control (IBAC) [11] models in order to represent the access control policy above.

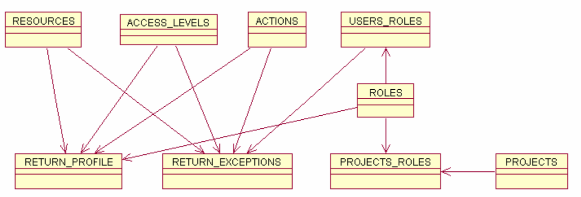


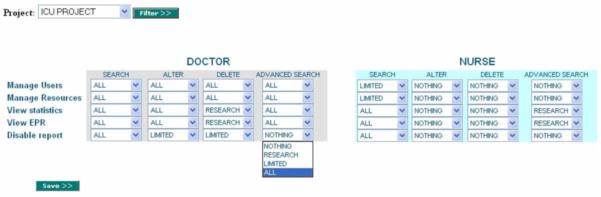
Figure 1. Entity-Relationship model

RBAC helps mapping generic actions and resources to groups of users, or the roles the users have within the Organization, allowing for easier management and implementation. Each resource has associated several actions and access levels for each action. According to what is defined for each role, a user profile is then collected each time a user tries to access the system. A user can have associated more than one role, and will inherit the privileges of all of them. The model is also divided in projects in the way that each project can have users associated to different roles, groups and resources.

IBAC is a Discretionary Access Control model, where the access control decisions are made according to the identity of the individual rather than the role he belongs to. This model allows for better granularity and is useful to create the exception rules specified within the policy, for instance as the one specified in item 2 above. This item says that only some specific doctors can access more sensitive information. This means that the role *doctor* has associated a set of generic privileges that do not include access to illness results such as cancer or HIV. A set of exception rules must be attributed separately to these users and, in this case, the users are the doctors that may have access to this type of sensitive information. The exceptions can add or take away privileges from the generic ones that are inherited by the user's roles.

The access control model was then implemented using a relational database system where all relations between the entities can be better described and in a modular way. To perform access control a centralized procedure is used. This procedure checks the roles to which users belong and collects resources, actions and access levels for those resources. It also intercepts the exception rules that user may have and, finally, returns to the user his/her complete authorization profile.

In order to associate resources and actions to roles and projects, a management tool was developed. This tool allows the administrator of a certain project to associate the roles and access permissions (including exceptions) for each user that he is responsible for. It is sufficiently generic and modular since it can be used for any application that needs to assign access rights to its users.



Project: ICU PROJECT

	DOCTOR				NURSE			
	SEARCH	ALTER	DELETE	ADVANCED SEARCH	SEARCH	ALTER	DELETE	ADVANCED SEARCH
Manage Users	ALL	ALL	ALL	ALL	LIMITED	NOTHING	NOTHING	NOTHING
Manage Resources	ALL	ALL	ALL	ALL	LIMITED	NOTHING	NOTHING	NOTHING
View statistics	ALL	ALL	RESEARCH	ALL	ALL	NOTHING	NOTHING	RESEARCH
View EPR	ALL	ALL	RESEARCH	ALL	ALL	NOTHING	NOTHING	RESEARCH
Disable report	ALL	LIMITED	LIMITED	NOTHING	ALL	NOTHING	NOTHING	NOTHING

Figure 2 . Management tool for the model

Having a model with these unique characteristics allows it to be flexible and modular and therefore, easy to add on other components.

3. The *Break The Glass* Policy

Traditional access control policies are usually very restrictive. The assumption is that users do not want to follow the rules, but rather would prefer to have unrestricted access to everything. Consequently, implementations focus mainly on avoiding and reacting to security breaches and not serving the user's needs and purposes.

As part of the access control policy stated in the previous section, BTG was included as a specific requirement defined by the healthcare professionals. This can be justified because there are situations when access is required, even if it means that patient confidentiality needs to be breached. The important issue is that this breach is known by the responsible parties and that the access is properly analysed afterwards. Then it can be considered whether the breach was well justified or was an intrusion.

With all these issues in mind, it was decided that policies with maximum freedom of access and, at the same time, maximum responsibility for any exceptional actions taken, are preferable to traditional ones.

Maximum freedom: the system must provide mechanisms for the users to access the requested information at all times, whenever it is needed.

Maximum responsibility: the system must provide mechanisms to show the user (who takes an exceptional action) an alert message making him aware that he is trying to access information he is not authorized to see. This makes him responsible for what he is doing and all the actions he may take afterwards; the system must provide mechanisms to notify all responsible parties and these notifications must be automatic. Note that such a mechanism requires a definition of the responsibility hierarchy for each department.

In the case of the VEMR system, users can search for information using the patient's process number. When they ask for information about a specific patient that they are not authorised to access, there is the need to verify whether the user is intending to *break the glass* by accessing information he is not authorized to.

The following are the steps needed in order to implement the BTG policy:

1. the user is authorized to access the system and then searches for information about a specific patient;

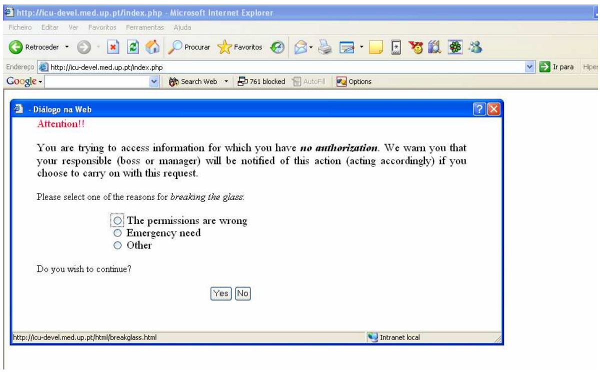
2. the authorization model verifies whether the user has access to the requested information;
3. the model returns *yes* or *no* according to the user profile; if it returns *no*, it shows the user that he can still access the requested information, by *breaking the glass*, but knowing that all his actions will be recorded and that non-repudiation mechanisms are in place (Figure 3);

4. the system is *frozen* until the user agrees or not with *breaking the glass*, and chooses a reason for doing it;

5. if the user *breaks the glass* the hierarchy model verifies who it needs to notify and proceeds with it;

6. all notifications and user actions are registered automatically.

The following figure (Figure 3) shows step 3 and 4 described above:


http://icu-devel.med.up.pt/index.php - Microsoft Internet Explorer
Ficheiro Editar Ver Favoritos Ferramentas Ajuda
Retroceder
Procurar
Favoritos
Endereço http://icu-devel.med.up.pt/index.php
Ir para
Google
Search Web
761 blocked
AutoFill
Options
- Diálogo na Web

Attention!!

You are trying to access information for which you have ***no authorization***. We warn you that your responsible (boss or manager) will be notified of this action (acting accordingly) if you choose to carry on with this request.

Please select one of the reasons for *breaking the glass*:

○ The permissions are wrong
○ Emergency need
○ Other

Do you wish to continue?

Yes No

http://icu-devel.med.up.pt/html/breakglass.html
Intranet local

Figure 3. *Break the Glass* process.

In terms of implementation, the process of searching for information about a patient needs to be complemented with an underlying request to the authorization infrastructure about the user's permissions. This is done with a procedure that checks the user's profile and the department where he works, and then decides to raise the BTG or not, depending upon whether access is denied or not.

There was no need to change the access control model implementation, but only to add some more information about departments and hierarchical relations when implementing BTG.

This was done by adding to the Entity-Relationship model (figure 1) one entity that related departments with users, and one that checked whether a department within the hospital uses the VEMR system.

Another important entity added was the one that described the hierarchical relations between the healthcare staff for each department, with information of the superior hierarchies as well as contact information for every one.

Finally, for the successful implementation of BTG, there is the need to implement proper tools to manage all the notifications in order for the non-repudiation service to fully work. This still needs to be finalized and properly tested.

These last features are very important, but also complex because they interfere with the organization's human processes and resources. Nevertheless, they are essential and allow for the policy verification, correction and process enhancement

4. Discussion

The BTG policy described in this paper was devised and developed according to the requirements for the environment in which it is being applied. There was a specific definition in the access control policy, by the security commission, that overriding rules should be provided.

However, what in theory may seem quite attainable may not actually be so when the tests start within a real environment. Unfortunately, the full set of tests is not available because the policy has not yet been fully implemented in the real system. Due to institutional constraints that still need to be overcome, the nurses are not yet using the system, only doctors can access the VEMR.

Nevertheless, there are already some issues that need to be discussed.

The BTG policy, if well structured and complemented with a set of mechanisms providing for non-repudiation (responsibility and notification), can be a simple solution to a very important problem in access control. After spending some time in a health care Institution we realized that this solution is sometimes used traditionally without the important characteristic of non-repudiation. The traditional *break the glass/door* policy in use allows a professional to have access to unauthorised information, by entering the medical records' room, and seeing whatever is there without any kind of restriction. The only way this professional can be punished is if someone sees him, and thinks that his behaviour is suspicious

Being implemented within a flexible and modular model, the BTG policy facilitated the integration and use of non-repudiation mechanisms.

It was possible to enlarge the model and adapt its infrastructure accordingly without much effort, so that additional features could be added. In some ways, this implementation helps to verify the policy and the model's flexibility and correctness.

Further work needs to be done concerning the definition and implementation of software to manage and update the hierarchical structure in an easy way. This is not trivial in a complex healthcare institution where people change their roles and departments quite often. Work still needs to be done in making sure the hierarchical structure in use is the most appropriate correct one.

Another important concern that needs to be tackled when the BTG policy starts to be used in the real setting is when and how this policy should be available. Should it be opened to everyone accessing the system regardless of their role, and should the non-repudiation mechanisms always be switched on? What if these non-repudiation mechanisms do not work because managers receive too many notifications and they do not even bother to check them? How are disciplinary actions to be applied and will they be defined according to the security breach level?

A balance must be found in all of this. The requests and successful break the glass attempts must be reduced to a minimum and under well justified situations. This must be tested properly before the policy is rolled out in a larger scale.

Finally, and as always, security is about human processes as well as technology. This is why the most difficult parts to implement are often not the technological ones but the ones related to people's processes and organizational structures.

The fact that the BTG policy was defined by the interested parties and the model adapted to the unique characteristics of the VEMR system, within a complex healthcare institution resulted in a complex but flexible infrastructure with simple functionalities and tools.

User intervention in the design and implementation of security policies and procedures is very important to its success, correct usage and further testing.

Acknowledgements

We thank the Security Commission of Hospital S. João for their collaboration and enthusiasm in order to develop and implement this project.

5. References

[1] Waegemann P. EHR vs. CPR vs. EMR. Healthcare Informatics Online. 2003. Available at: http://www.healthcare-informatics.com/issues/2003/05_03/cover_ehr.htm.

[2] Bakker Ab. Access to EHR and access control at a moment in the past: a discussion of the need and an exploration of the consequences. International Journal of Medical Informatics. 2004; 73:267-270.

[3] Anderson R. Security Engineering: A guide to build dependable distributed systems. Wiley 2001.

[4] Blobel B. Authorisation and access control for electronic health record systems. International Journal of Medical Informatics. 2004; 73: 251-257.

[5] Cruz-Correia R, Vieira-Marques P, Costa P, Ferreira A, Oliveira-Palhares E, Araújo F, Costa-Pereira A. Integration of Hospital data using Agent Technologies – a case study. AICommunications special issue of ECAI. 2005; 18(3): 191-200.

[6] Ferreira A, Correia R, Antunes L, Oliveira-Palhares E, Farinha P, Costa-Pereira A. How to start modelling access control in a healthcare organization. Proceedings of the 10th International Symposium for Health Information Management Research. 2005.

[7] Rissanen E, Firozabadi S, Sergot M. Towards a Mechanism for Discretionary Overriding of Access Control. Proceedings of the 12th International Workshop on Security Protocols, Cambridge. 2004.

[8] Povey D. Optimistic security: a new access control paradigm," in Proceedings of the 1999 workshop on New security paradigms. ACM Press, 2000; 40-45.

[9] Break-Glass – An Approach to granting access to Healthcare Systems. Joint security and privacy committee NEMA/COCIR/JIRA, International Medical Informatics. 2004. Available at: http://www.nema.org/prod/med/security/upload/Break-Glass_-_Emergency_Access_to_Healthcare_Systems.pdf. Accessed on: 14th March 2006.

[10] Ferraiolo D, Sandhu R, Gavrila S, Kuhn R, Chandramouli R. Proposed NIST Standard for Role-based Access Control. ACM Transactions on Information and systems security. 2001; 4(3):224-274.

[11] A guide to Understanding Discretionary Access Control in Trusted Systems. National Computer Security Center, Maryland. NCSC-TG-003, Version 1. 1987.