FI-OrBAC: a model of access control for federated identity platform

Farah LAYOUNI and Yann POLLET
Laboratoire CEDRIC
Conservatoire National des Arts et Metiers (CNAM)

ABSTRACT

In the information security field, the issue of access control is a crucial element. This access control is governed by a security policy that defines precisely the authorized actions for all actors in an information system. This step is necessary and constitutes a fundamental brick for the protection, confidentiality and integrity of information. This has more magnitude in the case of federated identity infrastructure (FII). In this article, we focus mainly on information and communication systems dedicated to the federated identity platform. We propose a new approach to treat the operational and security problems faced by an FII, particularly those related to access control and collaboration. The objective is to extend OrBAC with the concepts required to deploy and administer the model in distributed organizations. More precisely, the following problems have to be addressed: consistency of the access rules to be deployed, distribution of the access right control, distribution of the access right administration and characterization of the trusted components that need to be integrated in the global architecture to secure it.

Keywords

Federated identity, Circle of trust, Control access, Collaboration, Interoperability, ORBAC, FI-OrBAC

1. INTRODUCTION

The identity federation establishes a domain trust. It allows the interconnection of global information systems, facilities access to digital resources of another organisation or an external partner (eg commercial) and shares resources in a controlled and secure way. The identity federation manages an intranet/extranet for a population scattered around several systems. It allows companies with different technologies to share applications. Partners in a federated identity system depend on each other to authenticate their respective users and vouch for their access to services.

Such platform allows, for example [1], a traveler to combine flight booking, car rental and hotel reservation in a single operation. If the airline, the hotel and car rental use a federated identity management system, this means that they have a contracted mutual trust in each other's authentication of the user. The traveler could identify him/herself once as a customer for booking the flight and this identity can be carried over to be used for the reservation of a hotel room and for the renting of car.

So that companies can share applications without needing to adopt the same technologies for directory services, security and authentication. Federated identities can simplify network usage and enable new classes of applications, but they also introduce security worry, privacy risks and architectural challenges [2]. Establishing a federated policy between different organizations can be challenging. A successful federated connection depends on numerous configuration and policy details being setup correctly at both ends. The distributed entities face the problem of determining the degree of confidence to agree with each other. Traditional current approaches of confidence building assume that these entities know each others or must pass through trusted third party (TTP) or use an encryption technology [3]. But for FFI the challenge is even more difficult since the involvement of the user in the implementation of this confidence is indisputable. In such structure, the confidence is a question of personal valuation. It is submitted to an individual assessment which comes more from feeling and subjective than from technical guaranties provided by services providers. It is therefore necessary to propose ergonomics rules which place user in a reassuring position, i.e. he chooses the information he wishes to share, as many times as necessary.

In this way and through FFI, we propose to formalize these trust relationships by studying the following points: How to allow a user or an organization from one area to access resources in another area with the guarantee of having enough rights to perform its mission and only the minimum of necessary rights?– Defining a use case. – Studying the negotiation of security policies: how to ensure that security policy in an area does not compromise external securities? – Studying consider

how the user could control the dissemination of his attributes (identity, grade, location, function ...) between different areas.

So in this article and as part of a great project "FC2"[1], we try to establish a set of criteria that must fulfill our FII regarding effectiveness, interoperability, privacy and security in a complex context of multiple services and providers. We will focus in particular on security issues related to access control and collaboration among organizations making up the FII, and we propose an approach based on the model of access control OrBAC. This article is organized as follows: the second section resumes existing studies related to this domain. The third section presents our approach, detailing the components, operation and a scenario of execution. Finally, Section four gives the conclusions and suggests possible extensions of this work.

2. ACCESS CONTROL POLICIES

The management of trust and attribute release strategy rest on the implementation of a security policy that defines precisely the authorized or denied actions for all actors in a system. It is called control access policy. This section summarizes the existing solutions of control access policies and discusses their possible contribution to our outcome.

Access control defines authorization rules and constraints. To express the policies of access control, several formalisms have been proposed. The common feature of all models is the presence of the three following notions:

Object: An object is a container of information. The resources of a system (files, directories, e-mail,), and even information systems can be regarded as objects. An object is the target of an operation, it is a passive entity.

Operation/action: an operation corresponds usually to an elementary action as "read" or "writing". It is a way to access an object.

Subject: it is an entity that initiates operations on objects. Subjects include users of the system and processes implemented on behalf of those users.

Security policies, or more precisely their schedules permit, fall into two broad categories: discretionary policies (or DAC for Discretionary Access Control) [4] and mandatory policies (or MAC for Mandatory Access Control) [5]. In the discretionary model, permissions are granted to subjects according to their identity only. The mandatory model lean on the level of trust granted to subjects. Thus, if a subject is entitled to a certain level of trust, then he can access resources having an equivalent or lower security need. There are also variants of these policies that can better adapt to organizations, such policies based on the concept of roles (or RBAC for Role-Based Access Control) [6] or on the concept of teams (or TMAC for Team-based Access Control) [7].

In these models, we consider that a subject is granted permissions according to the roles he plays. Thus, in an organization, roles are defined and permissions are granted to those roles. Then the subjects were assigned to different roles and get the corresponding permissions. The RBAC [8] model operates on trading models rather than resources access. A role is a function within an organization. The basic principle of RBAC is that two users with similar roles have the same rights on the system. In this model, the concept of permission is primitive. It served as a basis for other languages.

However, the DAC, MAC and RBAC models are limited to expressing permissions. It is not possible to define explicitly bans and establish obligations. Hence the appearance of OrBAC model(Organisation-Based Access Control) [9] who is more oriented security policy. It is a model allowing abstract notions of users, action and object, expressing rights context, obligations or recommendations. It extends the expressiveness of access control systems through the integration of contexts into the models although this comes at the expense of the ease with which security properties of the system can be formally proved. OrBAC further extends this expressiveness by adding negative authorizations, obligations and recommendations. It contributes to define abstractions which allow us to relate managed objects to one another or which allow us to relate users, or groups of users, to groups of objects. We will present more details in the next section.

3. PROPOSED SOLUTION

This section recalls first the main concepts of OrBAC model and secondly the extension of this model in order to adopt it to our context.

3.1 OrBAC model

The main goal of OrBAC is to express security policy with abstract entities, and separate full representation of the security policy of its implementation by control access mechanisms. OrBAC [10] introduces the concept of organization and structures subjects, objects and actions, respectively, in roles (as in RBAC), views, and activities (as in TBAC: Task-based Authorization Con-

[1] http://www.fc2consortium.org/index.html

trols [11]). The central entity of this model is the organization; it can be seen as a group of subjects playing certain roles. For example in banking, an example of an organization can be the "credit unit". A subject can be either a user or an organisation. A role is an abstract representation of a group of users, for example, the role "Financial Advisor" and "administrator" can be played by users while the role "credit unit" can be played by organizations. Since the subjects play roles in organization, the relation "Empower" (org,s,r) means that organization (org) empowers the subject (s) to play the role(r). Also in this model, an activity represents one or more actions, and a view one or more objects. OrBAC also defines a notion of context as a specific situation that determines the validity of a rule. These concepts can be divided in two levels: concrete level (subject, action, object), abstract level (role, activity, view). The principal predicates [12] are as follows:

Permission (org, role, activity, view, context) $\wedge$
$Empower(org, subject, role) \wedge$
$Consider(org, action, activity) \wedge$
$Use(org, object, view) \wedge$
$Hold(org, subject, action, object, context) \wedge$
$=> Is\_permitted(subject, action, object)$

And the following schema summarizes all interactions between different predicates.

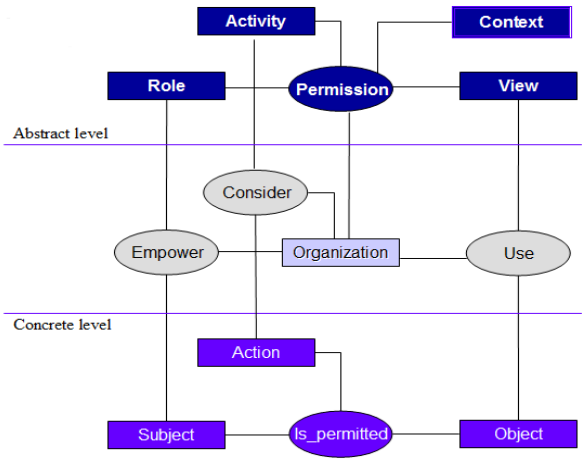

Figure 1: OrBAC interactions

One of the biggest advantages of OrBAC is that it offers mixed policy with permission, prohibition and obligation. With OrBAC, security policies could take into account context, entity abstraction, delegation and hierarchy.

In the context of the FII, we must not only specify the safety rules for each organization of the FII, but also manage the collaboration between these organizations. In such structure, the inter-organisational boundaries remain ambiguous. These borders are defined by the strategy of each organization to carry out the tasks entrusted to it, which leads to ask a number of questions: How to define a trans-organizational control access policy? How to specify a control access policy corresponding to each of the possible collaboration as respecting the authority of each organisation on its users and resources? How to minimize the effect of the internal structure of a circle of trust on the external cooperation? OrBAC is unable to reflect the complexity of organizations widely distributed and decentralized as well as the increasing diversity of access means to information. It can achieve the first point, to specify security policies for each organization, but it does not address the second problem. In fact, it is not possible to represent the rules involving several independent organizations belonging to a collaborative system in the same political OrBAC. Accordingly, it must be extended to meet the distribution needs, collaboration and interoperability between organizations.

3.2 Extension of OrBAC model to FI-OrBAC

Our model aims to construct and develop policies to implement protection mechanisms in access or electronic data exchanges, sensitive to availability, integrity, confidentiality such as in a FII. This implementation in a distributed environment supposes various additions to the existing model of OrBAC.

While authentication phase allows only verifying the identity of a user, the second service of a federated identity platform is to collect additional attributes for the user to manage access control or customize content. We have already proposed a solution [13] for the centralised attributes, especially when they are managed by the identity provider, through the manipulation of mobile agents but the problem that was raised is the case where the attributes are shared among different circles of trust and are managed by different organizations. We classify attributes under two types: Persistent attributes which define the identity of a person (Name, Age) and Evolution attributes which contain attributes considered relevant for each service. These attributes can customize the service and are not necessarily issued by the IDP to which the user is attached. These attributes are often managed by particulars institutions which are generally the source of their creation. For example, in the case of a student, his university may hold attributes as years of study, diploma and/or specialization. In federated identity architecture, these attributes are used to customize the service and especially to implement the delegation and the spread of attributes minimizing user intervention. This set of attributes requires switching between

the roles that a user can play in a society. To administer these attributes in the most implicit way, it is clear that the user must delegate some rights to these organizations so that they can deliver the attributes to the concerned service.To implement this idea, we needed to add additional predicates to the OrBAC model so that it can manage this distributed aspect. Fist we enrich this prototype by Delegate predicate: It illustrates the fact that the user authorizes an organism to represent him, confides temporarily power of decision to this organization. But the delegation must be ensured in a particular context and should be limited in time to ensure confidentiality and integrity of data. The context is usually the running of an application that will require certain attributes and the duration of the delegation depends on factors such as the nature of the act being delegated and the circumstances of the delegation. The actual duration of the delegation may be contingent on reassessment, be based on a specific time needed to spread and receive the required attributes by the service. The delegation also implies a frame to specify the rights associated with each attribute involved in this operation. Hence we introduce the second predicate Frame: It is a matrix associating with each attribute the right delegated by its owner. Each category attribute is associated with a quadruplet of rights: reading, writing, creation and deletion. The level of trust that can give a user to an organization can be implemented by specifying rights to attributes used under this delegation. Example of entries that can be found in such matrix (Fax ->read ..bank card number->read). Third, we have completed the model by the Detain predicate: the user uses the predicate to direct the federated application and more specifically the agent responsible for the execution to the organization that owns the attributes sought. So in chronological order, the user must firstly use this predicate to redirect application to the organisation able to provide the missing information and then delegate to this institution the essential role while specifying the rights for each attribute through the frame.

In the following, we present both syntax and semantic of these additional predicates:

- Delegate(s,org,r,c,f), over domains Subject*Org*Role *Context*Frame, s as subject, org as organization, r as role and c as context=>Delegate means that subject s entrusts his role r to the organization org in the context c under the frame f

- Frame(As,R), over Attributes*Rights, As as attributes and R as rights=>Frame represents the matrix which specifies access rights for each attribute. These rights covered through this frame are: Reading attributes(r), Writing on attribute(w), Creation of an attribute (c), Deletion of an entry (d)

- Detain(org,As), over Org*Rights, org as organisations and R as Attributes=> Detain means that organization org detains attributes As

$\forall org \in Org, \forall s \in Subject, \forall r \in Role,$
$\forall as \in Attributes, \forall f \in Frame, \forall c \in Context,$
$\forall R \in Rights, \forall o \in Objects, \forall A \in Action,$

Delegate(s,org,r,c,f)$\wedge Frame(As, R) \wedge$
Detain(org,As)=>Ispermitted(s, A, o)

3.3 exemple

We turn now to illustrate these predicates through an execution scenario: we will take the example of registering in a day-nursery. Usually many papers and documents are required for this service. So it is interested to provide this service online, a real benefit for working parents who do not have enough time to look for different supporting documents.

As illustrated by following figure, the DN day-nursery offers the Web service WS, and Bob wishes to invoke this service WS in order to register his son online. The first step consists of verifying the identity of Bob. This is assured by sending a mobile agent [14] to the IdP to which the user refers to check the Persistent attributes. But our study concerns the second step of collecting evolution attributes. To finalize registration, Bob has to provide at least these papers: proof of address (e.g. EDF invoice), Identification Card for the two parents or family record book, declaration of pregnancy or birth certificate of baby, the two last payslip of the two parents.

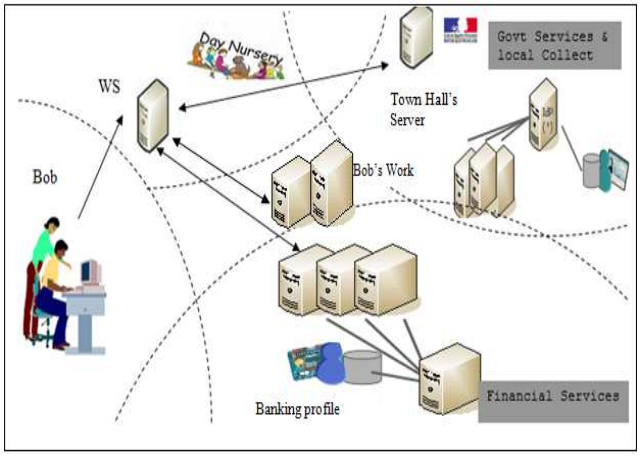

Figure 2: inclusion in the nursery

Supply these papers is difficult, and this is where our

model FI-OrBAC intervenes. Thus Bob must delegate the day-nursery his role of citizen in the context of registering his son :
Delegate (Bob,DN,Customer,Registering_son,Fp).

First, the user has to specify where these attributes will be available. In our case, the family record book is disposable in the Hall town: Detain(DN, Town Hall's server),
Detain(EDF, proof of address),
Detain(bank1,IBAN),
Detain(Bob'swork, payslip),
Detain(EDF, EDF_invoice).

Second, there is the phase of delegation. Bob has to delegate his role of employee to the organism where he works so that it can transmit the payroll to the nursery:
Delegate(Bob, Bob's work, employee, playslip_transmission, Fp1) ; Fp1(playslip->read).

It will be same with bank, Town Hall and Edf Group for delegating his role to the bank to pay the cost of registration, providing payslip, providing EDF invoice :
Delegate (Bob, EDF Group, Citizen,
EDF_invoice_transmission, Fp2); Fp2(EDF_invoice,read)
Delegate (Bob, Town hall, Citizen, family_record_book, Fp3); Fp3(,read)
Delegate (Bob, Bank, Customer, fee_paying, Fp4); Fp4(Card number,read)

With the use of this extension of OrBAC especially these three predicates, we have succeed in representing the rules involving several independent organizations belonging to the federated platform. We have resolved the problem of access control when the needed attributes are distributed among several circles of trust. We have succeeded in adapting model to distributed context and especially involve the user in the implementation of the access policy.

4. CONCLUSION AND FUTURE WORK

This article introduces a new security approach that meets the needs control access and collaboration of a FII. FI-OrBAC manages collaboration between organizations through a federated identity service, while controlling the interactions between these organizations are in line with their expectations and internal policies. It is easily applicable to this multi organizational context because it imposes no limitation on the number or size organizations (passage to scale), and it may define an extensible and flexible security policy (managing change in organizations). The coupling between the organizations is low (loose coupling), and each organization contains its own resources, services, applications, operating system, operating rules, objectives and rules of security. It is not necessary to know the hierarchical structure of others organizations, thus provides data confidentiality and the way in which services are implemented. This approach can be extended by studying other problems related to the integrity and availability of data and tolerance mistakes. With regard to availability, you can specify for example the obligation to provide adequate resources for performing a specific activity under particular events (failures, reconfiguration, etc.). On integrity, we can integrate control flow of information, and define different levels of criticality for data and organizations.

5. REFERENCES

[1] D. Temoshok, "Federal e-authentication initiative: Federated identity and interoperability." Liberty Alliance Meeting with Japanese Government, October 18, 2004.

[2] E. Maler and D. Reed, "The venn of identity: Options and issues in federated identity management." IEEE Security and Privacy magazine, March-April 2008.

[3] E. S. D. I. . Information, "The concept of trust in network security." Entrust White Paper, August 2000.

[4] J. Carole S, "Guide to understanding discretionary access control in trusted systems." NCSC-TG-003, September 1987.

[5] D. E. Bell, L. J. L. Padula, and M. C. B. MA, "Secure computer system: Unified exposition and multics interpretation." NCSC-TG-003, Technical Report ESD-TR-75-306, MTR-2997, Rev.1, Bedfort, MA.

[6] R. Sandhu, E. Coyne, H. L. Feinstein, and C. Youman, "Role-based access control: A multi-dimensional view." In Proceedings of the 10th Conference on Computer Security ApplicationsIEEE Computer Society Press, Los Alamitos, CA, 54-62, 1994.

[7] T. A. Fahad and J. CHEN, "A model for team-based access control." IEEE Computer Society, Las Alamitos CA, ETATS-UNIS, 2004.

[8] R. S. Sandhu, "Role-based access control." Advances in Computers Academic Press, 1998.

[9] A. Abou-El-Kalam, S. Benferhat, A. Miege, R. E. Baida, F. Cuppens, C. Saurel, P. Balbiani, Y. Deswarte, and G. Trouessin.

[10] F. Cuppens, N. Cuppens-Boulahia, and A. Miège, "Héritage de privilèges dans le modèle or-bac : application dans un environnement réseau." SSTIC, rennes FRANCE, 2004.

[11] R. Thomas and R. Sandhu, "Task-based authorization controls (tbac): A family of models for active and enterprise-oriented authorization management." 11th IFIP Working Conference on

Database Security, Lake Tahoe, California, USA, December 1997.

[12] M. B. Ghorbel, F. Cuppens, N. C. Boulahia, and A. Bouhoula, "Managing delegation in access control models." 15th International Conference on Advanced Computing Communication ADCOM, December 2007.

[13] F. Layouni and Y. Pollet, "Use of mobile agents in a federated identity structure." The IACIS 48th Annual International Conference, Savannah, Georgia, USA, October 2008.

[14] ——, "Ontology for mobile agent cooperation in federated identity platform." aswc2008, Bangkok Thailande, December 2008.