Universitat Autònoma de Barcelona

Departament d'Enginyeria de la Informació i de les Comunicacions

Contributions to access control: Continuous access and attribute-level interoperation

Submitted to Universitat Autònoma de Barcelona
in partial fulfillment of the requirements for the
degree of Doctor of Philosophy in Computer Science

by Carles Martínez García

Bellaterra, July 2011

Directed by

Dr. Guillermo Navarro Arribas

and Dr. Joan Borrell Viader

We certify that we have read this thesis and that in our opinion it is fully adequate, in scope and in quality, as a dissertation for the degree of Doctor of Philosophy.

Bellaterra, July 2011

Dr. Guillermo Navarro Arribas
(Principal Adviser)
Dr. Joan Borrell Viader
(Adviser)

Committee:

Dr. Josep Rifà Coma
Dr. Joaquin García
Dr. Óscar Cánovas
Dr. Javier Herranz (substitute)
Dr. Joan Arnedo (substitute)

If we knew what it was we were doing, it would not be called research, would it?
(Albert Einstein)

Abstract

Computerized access control is founded on some assumptions that limit its application in concrete environments. First of all, the standardization of access control models built on a poor understanding of access. Access has been historically considered binary in the sense that access is permitted or it is not. However, there are operations that can be executed through a variable execution level. That is the case of QoS-subjected actions, for example, where the resources put on serving an access conditions the quality of the access itself. As quality of access is, indeed, an access control regulation, the access decision could be formulated in terms of the authorized access level rather than through simple permit/deny decisions. A second assumption lies in the form in which users are related with authorization-relevant information. Authorization-relevant information are facts like who the user is, which characteristics the user has or what the user owns. However, this information may be parametrized. Uncertainty, trust, seniority or risk are just few examples. This semantics should be taken into account along the authorization process. In this thesis we present FRBAC, an access control model which breaks with this two assumptions, and we demonstrate its applicability in different scenarios, paying special attention to the multi-domain environment. We also propose a collaboration mechanism which enables the interoperation between heterogeneous access control models and it is compatible with FRBAC.

Els models de control d'accés es fonamenten en dos pilars –entre d'altres– que limiten el seu àmbit d'aplicació. El primer d'ells tracta en la forma en la que els accessos són entesos. Històricament, els accessos han estat considerats estrictament binaris. L'estandardització dels models de control d'accés es va centrar únicament en permetre o no els accessos en comptes de determinar les condicions d'accés. No obstant, els accessos poden ser entesos a través d'una visió més rica que la binaria. Data Lying és un bon exemple, on el nivell de veracitat en les consultes a una base pot ser modificat tenint en compte atributs associats als usuaris, entenent major nivell d'accés com major veracitat a les respostes obtingudes a una mateixa acció. El segon pilar tracta en la forma en que els usuaris són relacionats amb informació rellevant al procés d'autorització. Els usuaris són autoritzats en base a qui són, quines característiques tenen o quines coses posseeixen. No obstant, darrera d'aquests fets es poden trobar altres semàntiques els models de control d'accés han de ser capaços d'interpretar. La certesa en dita informació i la confiança en l'usuari són bons exemples. Aquestes semàntiques poden ser útils per determinar el nivell d'accés que tenen els usuaris. En aquesta tesis presentem FRBAC, un model de control d'accés que trenca amb aquestes suposicions inicials, i demostrem la seva utilitat en diferents escenaris, prestant especial atenció als escenaris multi-domini on es proposa també un mecanisme de interoperabilitat a nivell d'atribut compatible amb FRBAC.

Los modelos de control de acceso actuales parten de dos asunciones –entre otras– que limitan sus ámbitos de aplicación. La primera de ellas reside en la forma en la que se entienden los accesos en sí. Históricamente los accesos se han considerado estrictamente binarios (se permiten o no), cuando estos pueden ser entendidos a través de un nivel continuo de acceso. Data Lying es un buen ejemplo, donde el nivel de veracidad obtenido en las consultas a una base de datos puede ser alterado en función del historial del usuario, entendiendo mayor nivel de acceso cuanto mayor veracidad en los resultados de una misma acción. La segunda asunción trata en la forma en la

que los usuarios son relacionados con la información útil en el proceso de autorización. Los usuarios son autorizados en base a quienes son, que características tienen o que cosas poseen. Sin embargo, detrás de estos hechos pueden esconderse otras métricas que los sistemas deben interpretar. La veracidad de dicha información es una de ellas. Estas métricas pueden ser usadas para determinar el nivel de ejecución de las acciones que llevan a cabo los usuarios. En esta tesis presentamos FRBAC, un modelo de control de acceso que rompe con estas asunciones y demostramos su utilidad en diferentes entornos, prestando especial atención a los entornos multi-dominio para los que se propone también un mecanismo de interoperabilidad compatible con FRBAC.

Acknowledgements

Si avanzar es desaprender, ¿cómo iba a haber otro final?

He caminado desde la playa hasta lo más alto en la corona de esta torre medieval. Desde aquí casi puedo tender la mano sobre el pueblo de Caldes d'Estrac que yace bajo mis pies. He paseado por sus calles, he oído las campanas de su iglesia repicar, he dejado escurrir entre mis dedos el agua que brota de la fuente termal. He visto las siluetas blancas, de la princesa y sus sirvientes, que todavía habitan la torre *dels Encantats*. He podido contemplar el azul que baña las costas de la comarca. Costas teñidas a base de pino y encina por un bosque mediterráneo que se extiende más allá *dels Tres Turons*. He podido saludar las barcas de pescadores que se mecen a lo lejos, y por la noche parecen pequeñas estrellas caídas a la mar.

Buscando un remanso de tranquilidad para escribir esta tesis, me aislé en la comarca del Maresme. Hoy quiero aislarme en esta tesis para explicar lo que la comarca me ha podido enseñar. He caminado desde la playa hasta la corona de esta torre medieval, y en lo más alto, contemplando este paisaje igual que contemplo este final, sólo puedo preguntarme si lo que veo es lo que tengo delante, o lo que ya dejé atrás.

Empecé este doctorado desnudo ante el papel, sin conocimiento alguno sobre el tema que iba a tratar. Recuerdo haber leído con curiosidad un capítulo de un libro para poder empezar: "El control de acceso es el proceso de mediar cada petición de acceso, sobre recursos albergados en un sistema, y determinar si el acceso debe de ser permitido o denegado". Parecía razonable y acepté esa definición. Hoy, después de

cuatro años, a tan sólo unos días para acabar, no hago más que cuestionarla [1]. Tal vez sea tarde para rectificar. El tiempo me arrastra hasta el fin de este doctorado, y ya sólo me queda disfrutar de este final, convencido de que no hay mejor forma de acabar.

Algo habré aprendido en el camino, no sé. Tal vez la mayor enseñanza de este *Doctor Philosophiae* sea aprender a cuestionar lo que se da por supuesto. Lo que se da por sabido. A cuestionar lo que he podido aprender. A cuestionar lo que he podido enseñar. Tal vez la mayor enseñanza sea no temer a cuestionar los senderos trazados desde su inicio. No temer a trazar nuevas estelas en la mar, y cuestionarlas como el que más. No temer a ser crítico con las opiniones de los demás. Tal vez la mayor enseñanza sea comprender que lo que entiendo hoy no tiene por que ser lo que entienda mañana. Tal vez la mayor enseñanza sea que contradecirse en el tiempo es, sin duda, una forma de evolucionar.

Hoy comprendí la moraleja. Caminar, conocer, entender. Eso es desaprender. Ya en la Antigua Grecia sabían que el tratar de comprender el mundo que nos rodea, plantea muchas más preguntas que preguntas es capaz de responder. Basta con mirar a nuestro alrededor y darse cuenta de que lo más elemental, aquello que conforma todo, guarda grandes preguntas por responder. Basta con mirar al cielo infinito una noche estrellada para sentirse abrumado por los misterios de ese universo que nos cobija. Basta con volver a bajar la mirada para preguntarse cómo hemos llegado hasta aquí.

Concluyendo estas líneas delante de un paisaje de mar, sólo puedo preguntarme si lo que veo es lo que tengo delante, o lo que ya dejé atrás. No cabe rectificar. No cabe volver a empezar. Este doctorado está a punto de acabar, y me voy convencido

[1] Hoy entiendo el control de acceso como algo mucho más general. Regular los accesos a los recursos del sistema, y ya está. Antes, durante o después de que sucedan. Adaptando las condiciones de acceso y no limitándose a permitir o denegar. Así funciona en el mundo real. Basta con pasear por la calle y ver una señal de tráfico, basta con entender el canto de los pájaros en un bosque, basta con ojear el código penal.

de que sólo los pasos que he dado me podrían haber traído hasta aquí. Así es el final. Sólo podría irme con más preguntas de las que vine. Ya aprendí a cuestionar todo lo que leí. Ya aprendí a cuestionar todo lo que he escrito. Si caminar es desaprender, no hay mejor manera de terminar. Lo que sigue a estas páginas es sólo el trabajo que ya se me antoja pasado. Una pequeña parte de estos últimos cuatro años donde todo lo aprendido no tiene ni introducción, ni nudo. Ni final.

Quiero agradecer el soporte recibido por mi familia y amigos durante estos cuatro últimos años en especial. Agradecer a esos ojitos azules, que brillan hasta en la oscuridad, e iluminan un camino que ha valido, y vale, la pena caminar. Agradecer a mis compañeros becarios por ser algo más que simples compañeros. Os echaré de menos. Agradecer al personal del departamento y al grupo SeNDA en particular. Agradecer, como no, a Guillermo Navarro, Joan Borrell, y al resto de coautores de los artículos, por el soporte recibido a lo largo del doctorado. Parroquia, ha sido un placer. Gracias a todos. Por todo, gracias.

Partial support by the Spanish MICINN (projects TIN2010-15764, TSI2007- 65406-C03-02) and Universitat Autònoma de Barcelona (PIF 472-01-1/07) is acknowledged.

Contents

Chapter 1

Introduction

From territorialism to RBAC: origins of access control

The need to control the access to something is as old as the ability to assess it. Access control is a primitive behavior born fueled by the survival instinct. Before the first hominids, some species determined simple rules on the usage of shared resources. One of the first manifestations of this behavior was territorialism, where groups, or individuals, settled in a marked area and defended it against intrusions [17] usually by individuals with similar hunting habits. In its initial form, access control was dissuasive, since nothing prevented an intruder to access a restricted area but the threat of being punished if discovered.

The human evolution, and the development of technologic skills, led to a new understanding of authorization: restrictive access control. Physical barriers as walls, locks and pits prevented unauthorized accesses before they were done, acting as a gateway between users and resources. At the same time, the development of social skills led to a richer understanding of restrictive access control, determining the conditions on the usage of protected resources, and penalties in case of misuse, rather than simply preventing accesses by unauthorized principals. Both visions of access control accompanied the human evolution combining restrictive and dissuasive access control paradigms at the same time. Restrictive access control was mainly focused on

physically preventing unauthorized accesses to protected resources, while dissuasive access control was focused on determining the conditions of the resource usage.

The development and popularization of information technologies led to the emergence of access control in computer environments [24]. The nature of computer environments favors an exhaustive and a priori control of all the accesses taken in the system, providing a gateway between users and resources in order to regulate every access. Despite in the physical world, access control remained being dissuasive and restrictive, computer environments adopted an essentially restrictive vision of authorization. At the beginning, computerized access control mechanisms simplified the restrictive authorization model deployed by the society and focused on just determining who could access every resource, rather than determining the way in which the resources could be accessed.

It was the deployment of multiuser computer environments which fueled the popularization and evolution of computerized access control. Identity-Based Access Control was the first iteration. Access control lists dictated the authorized users to access every resource [24]. As computer environments grew in complexity, and the number of users and resources grew, Identity-Based Access Control became unmanageable and new paradigms arose trying to break its complexity [34]. Discretionary Access Control [18] shifted the management of authorization lists to the owner of every resource, splitting the management complexity through the decentralization of the process. The Mandatory Access Control [3] paradigm applied to environments where the authorization management must remain in a central authority. The growing complexity of computer environments continued fueling the need for reducing the complexity of the authorization management.

User abstraction became an effective way to reduce the complexity of the authorization management, allowing to refer to users based on their common characteristics rather than their unique identity in the system. The increasing complexity and expressivity of access control lists made them evolve to more complex access control policies. Groups were one of the first user abstraction mechanism, that applied in

both, the Mandatory and the Discretionary Access Control paradigms. In the Mandatory access control paradigm, where the policy management remained in the central authority, user abstraction was specially necessary to reduce the complexity of management. Multilevel Access Control [1] profiled users through security levels. Then, access permissions were assigned to security levels rather than users themselves. Following this direction, appeared the Role-Based Access Control model (RBAC) [15].

The incursion of IT technologies in business processes popularized RBAC. Role-Based Access Control is an access control model designed to accommodate organizational access control policies. In RBAC, the privileges that users have are not related with the users' identity but the roles that users play. Users are granted with roles depending on their function inside the organization. At the same time, every role is assigned with different permissions which allow the role members to carry out the functions that they are supposed to do. Users acquire the privileges assigned to the roles they play. Hierarchical relations between roles increases the expressivity of the model, allowing senior roles to inherit privileges from the junior ones, helping in the reduction of the policy management complexity.

In parallel, from the impossibility to plan in advance the legitimate accesses in complex systems, arose the principle "Make the user ask for forgiveness not permission" [6]. This principle tried to enforce computerized access control with dissuasive measures rather than restrictive ones. In other words, a priori access control decisions were substituted by a posteriori punishment measures in case of an improper access. This principle applied to environments where the damage of improper accesses could be undone or, at least, quantified and compensated [33]. However, the impossibility to apply this access control paradigm in risky environments, such as economic ones, led the paradigm to a lack of support by the community.

Nowadays, the growth and recent advances in distributed systems and computer networks not only enable the decentralization of computer environments but also existing systems and services to interact in order to provide new and improved applications [19]. The interoperation of independent systems such as those in the health-care

industry, public administration and business can result in new functionality and cost savings. With this interoperation comes the need of ensuring a consistent interpretation of the access controls across the heterogenous systems and shared resources. Many proposals enable interoperation of independent access control systems, and it is still an active research issue.

In parallel to distributed systems, the incessant advances in communication and computation technology have fueled the grown of novel applications which moves away from the isolated system paradigm towards an environmental integration of them. Promoted by the growth of this novel applications, comes up the need for a context awareness in the authorization process in order to protect the application's resources. Context-aware access control aims to describe access control policies taking into account the state of the environment and the users' privileges in order to issue the access control decisions. The need to relate the authorization process to the context state has fueled a research effort, which is still active.

Shortcomings of the current access control

Computerized access control is founded on some assumptions that limit its application in concrete environments. First of all, the standardization of access control models builds on a poor understanding of access. Access has been considered binary (you can access or you cannot) while in some cases it can be understood under a continuous interpretation. This principle allows, for example, in the physical world, a novice driver to access the highway at a maximum speed of 80 km/h, senior drivers to use the highway at 110 km/h, and autocycle drivers not to access the highway. Back to the computer environments, there are operations that can be executed through a continuous variable access level. That is the case of Quality of Service (QoS) [13], for example, where the resources put on serving an access conditions the quality of the access itself. As quality of access is, in the end, an access control regulation, the access decision could be formulated stating the authorized access level rather than

through simple permit/deny decisions.

A second assumption lies in the form in which users are related with the information which is relevant in the authorization process. Authorization-relevant information are facts like who the user is, which characteristics the user has or what the user owns. However, in concrete environments, this information may be parametrized. Uncertainty on the authentication process, user trustworthiness, user seniority or risk are just few examples. This phenomenon can be clearly observed in the multi-domain environment, where security-relevant attributes related to the users are translated between the different domains in order to enable the interoperation. The intrinsic imprecision in the conversion process leads to uncertain authorization-relevant information, which is best addressed in an explicit way [9] at the access decision time. The parametrization of authorization-relevant information should be taken into account along the authorization process and must be forwarded towards the access decision.

Objectives

In the following lines, the specific objectives of the thesis are listed:

- Propose a generalization of RBAC with the following characteristics:
  - **Access level**: The proposed model must be able to issue access control decisions stating the authorized access level rather than simple permit/deny decisions. Access control decisions of the form permit/deny must be also contemplated in order to guarantee the compatibility with RBAC. This objective includes the study of the different possibilities enabled by a continuous interpretation of access.
  - **Parametrized assignments**: The user-role and role-permission assignments in the proposed model may represent semantics beyond the simple fact that a user or a permission is assigned to a role. This parametrizing semantics will allow to capture, among others, uncertainty, trust or risk on the assignments.

  - **Fine-grained access control policies**: The very definition of RBAC sometimes leads the model to a too coarse-grained access control policies. Little changes in the user-role or role-permission assignments can lead to dramatic changes in the privileges assigned to the users. The proposed model must be able to accommodate more fine-grained RBAC policies.

- Propose a mechanism which enables the interoperation of independent systems in the multi-domain environment, with the following characteristics:

  - **Generic**: The mechanism must enable the interoperation of independent systems with heterogeneous access control models.
  - **Scalable**: A transversal problem of interoperability is the complexity of the process as the number of domains grows. The proposed mechanism must be scalable.

Structure

This thesis is presented as a compendium of publications. Chapter 2 introduces the publications taking part of the thesis showing the argumentative thread that waves them. After a little introduction, the articles that take part of the compendium are referred. Chapter 3 summarizes the main contributions, expand some concepts, and discusses the applicability of the contributions. Finally, Chapter 4 concludes the thesis. We refer to the published articles, placed in the appendices, to find concrete background on the topic and the related work.

Chapter 2

Contributions

In this chapter we introduce the contributions of the thesis, showing the argumentative thread that weaves it as a whole. After a little introduction, we refer the articles of the compendium. The concrete background and the related work of every contribution are placed on the corresponding articles.

The first contribution of this thesis is FRBAC (Fuzzy Role-Based Access Control). FRBAC is a generalization of RBAC founded on fuzzy relations which enables the description of parametrized user-role and role-permission assignments. The multivalued user-role and role-permission relations allows to describe semantics in the assignments beyond the fact that a user belongs to a role or a permission is assigned to a role. User trustworthiness, user seniority, uncertainty or risk involving the assignments are just few examples. FRBAC allows to forward this parametrization and take it into account at the access decision time.

FRBAC proposes a new understanding of access and, thus, a new understanding of the access decisions. The standardization of access control models builds on a poor understanding of access. Historically, access has been considered as something binary, when it may be not. There are environments where accesses can be performed through different access levels, and the access control mechanism should determine

the authorized access level for a request, rather than just permit or deny the execution. FRBAC issues access decisions in the range $[0, 1]$, stating the authorized access level that users have over resources through operations. Parametrized assignments links nicely with the notion of access level. Rather than reasoning over multivalued information and issuing binary access control decisions, the access level can be adjusted to the semantics of the assignments. This represents a new understanding of accesses and opens new applications fields which will be discussed in Section 3.1.3.

At this point, we encourage the reader to goto the article "C. Martínez-García, G. Navarro-Arribas, and J. Borrell, Fuzzy role-based access control, Inf. Process. Lett., vol. 111, pp. 483–487, April 2011." Appendix A, for a better understanding of the thesis.

FRBAC defines access control decisions in the range $[0, 1]$. In the following paper, we depart from FRBAC to propose the concept of polymorphic permissions, in order to describe an intra-role user progression model inspired in role-playing games. The multivalued nature of the assignments of FRBAC allows to describe a user progression within the roles. The more strength in the user-role assignment, the more a user plays a role. An increasing strength of the user-role assignment increases the strength of the user-permission assignments, which will lately result in progressive abilities acquisition and progressive abilities enhancing, two concepts widely adopted in computerized role-playing games.

At this point, we encourage the reader to goto the article "C. Martínez-García, G. Navarro-Arribas, and J. Borrell, Intra-role progression in RBAC: An RPG-like access control scheme. Accepted for publication in the 4th International Workshop on Autonomous and Spontaneous Security (SETOP), 2011" Appendix B, for a better understanding of the thesis.

We now leave the RBAC domains to talk in terms of Attribute-Based Access Control (ABAC) [38]. We consider attributes as any authorization-relevant information referred to by an access control policy, ranging for example, from an identifier to a role, or more generic attributes such as age, regardless of the underlying access control model. This approach provides a simple abstraction for a variety of access control models ranging from RBAC to more general discretionary access control.

When two or more organizations decide to cooperate, there is a clear need to control the access across the interoperation scenario. We consider attribute conversion as the most promising one. Attribute conversion aims to establish similarity relations between the authorization-relevant information that characterizes users in the different domains. Due to the heterogeneity of the domains, in the general case it will be difficult to find absolute similitude between attributes. We propose an interoperation mechanism that deals with the intrinsic imprecision involving the attribute conversion process. This imprecision links with parametrized user-role assignments of FRBAC and the multivalued access decisions.

In the following paper we describe a generic attribute conversion mechanism which enables the interoperation not only between heterogeneous systems, but heterogeneous access control models, generalizing them trough ABAC. We also study the scalability issues involving the interoperation. The compatibility between FRBAC and the attribute conversion mechanism is discussed in Section 3.3.

At this point, we encourage the reader to goto the article "C. Martínez-García, G. Navarro-Arribas, S. N. Foley, V. Torra, and J. Borrell, Flexible secure inter-domain interoperability through attribute conversion, Information Sciences, vol. 181, no. 16, pp. 3491 – 3507, 2011." Appendix C, for a better understanding of the thesis.

The attribute conversion mechanism has been applied to enable access control in the multi-domain environment described by MedIGS [37]. MedIGS is a multi-agent-system middleware with the purpose of data sharing between medical institutions.

Its main objective is the creation of a virtual electronic patient record, which is the collection of all the medical documents referring to a given patient, located in any of the hospitals that takes part in the scenario. This last contribution shows a practical example of the applicability of a subset of the attribute conversion mechanism.

At this point, we encourage the reader to goto the article "C. Martínez-Garcia, G. Navarro-Arribas, J. Borrell, and A. Martín-Campillo, An Access Control Scheme for Multi-agent Systems over Multi-DomainEnvironments, in 7th International Conference on Practical Applications of Agents and Multi-Agent Systems (PAAMS 2009), 2009, pp. 401-410." Appendix D, for a better understanding of the thesis.

Chapter 3

Discussion

In this chapter we summarize the contributions of the thesis and discuss their applicability.

3.1 FRBAC

FRBAC is an access control model which generalizes RBAC through fuzzy relations. In RBAC, the fact that a user, or a permission, is assigned to a role has a clear interpretation: due to the user duties within an organization, the user needs to play some roles, and the role members need to carry out specific functions within the system, represented by permissions. Users acquire the permissions related to the roles they play. Unlike RBAC, where user-role and role-permission relations are crisp, FRBAC defines user-role and role-permissions as fuzzy relations in the range $[0, 1]$. The fuzzy relations enable the parametrization of the assignments, which are application-dependent and may have different interpretations. The multivalued nature of the user-role and role-permission relations may specify something more than simple membership degree. Few examples on the semantics of user-role assignments may be user seniority, user experience, user trustworthiness, and uncertainty or risk involving the assignments. Role-permission relations may represent different semantics than user-role

assignments, as risk, need to use of the permissions, or average trustworthiness of the role members.

The user-permission relation in FRBAC arises from the aggregation of the user-role and role-permissions relations, and determines the degree in which users own permissions. This degree is also expressed in the range $[0, 1]$ and determines the access degree that every user has over every permission. It is noteworthily to say that the semantics of the user-role and role-permission assignments must be coherent between them in order to enable their composition. Intuitively, it makes no sense to aggregate user seniority on the user-role assignment with the risk involving the role-permission assignment. However, it may be possible to specify the user-role assignment risk based on user seniority. In this way, both the user-role and the role-permission assignment could be aggregated to determine, in this particular case, the risk involving the relation between users and permissions. All the parameters involved on computing the user-role and role-permissions magnitude must be reduced to something that will be lately composable to determine the user-permission relation.

3.1.1 Access level, continuous access and polymorphic permissions

FRBAC determines the access level, in the range $[0, 1]$, that users have over permissions. The user-permission strength determines the access degree that users have over objects through operations. There are three different interpretations of the user-permission strength: continuous access, polymorphic permissions and thresholded plain permissions.

Continuous access

Access has been historically considered binary: you can open a door or you cannot, you can transfer money or you cannot, you can read a medical record or you cannot. While there are accesses that clearly have a binary interpretation –in the general case

it makes no sense to half-open a door–, some other accesses may have a continuous interpretation. Imagine a video-on-demand service regulated through a QoS policy which prioritize premium users. The access to the videos offered by the service is granted to regular and premium users, however the resources put on serving the premium users guarantees higher quality standards than the offered to regular users. In this scenario, access control decisions does not only determines whether a user is allowed or not to access the service, but the access control decision determines the access degree, which will lately condition the quality of the access itself.

Access control policy description languages, such as Ponder [11], Keynote [7] and XACML [31], and the certification standards SAML [26] and SPKI [14] provide mechanisms to determine the conditions under which accesses must be permitted. Despite conditions are not defined in the RBAC standard, the RBAC profiles of the cited mechanisms allow to include conditions in the definition of permissions. Conditions enable, for example, to constrain the execution of a permission in a given time interval or limit the maximum amount of money that users are able to transfer, allowing to describe context-aware and fine-grained RBAC-like access control policies.

The purpose of conditions must not be confused with the idea of continuous access. Conditions are a mechanism that builds on a binary interpretation of access and provides the access control policies with more expressivity, constraining the execution of permissions that users have obtained by virtue of the roles they play. Access control decisions continue being of the form permit/deny. Continuous access, however, builds on a reinterpretation of accesses. Accesses are not just executed or not, but accesses can be executed through a variable strength level and it is the decision point which determines the execution strength that users have over resources through operations. The access level can be enforced transparently to the user. The user accesses the resource and the system adapts to conditions of the access.

The access decisions of FRBAC have a direct mapping with continuous access, where 0 means the minimum access degree –normally *null*, but other interpretations

may apply– and 1 means the maximum access degree. The interpretation of continuous access depends on the application itself, not on the operation or the object being accessed. Figure 3.1 shows an example of access level.

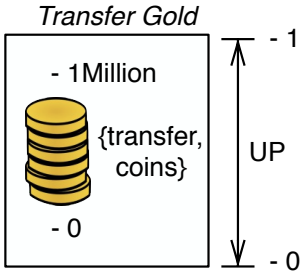

Figure 3.1: Access level representation. The user-permission magnitude determines the access level that every user has over the object. In this case, the user-permission magnitude determines the amount of gold coins that every user is allowed to transfer.

Polymorphic permissions

Another interpretation of access level is given by polymorphic permissions. The user-permission assignment degree may not always refer to the execution degree of an action. Depending on the user-permission strength, permissions will relate different operations and objects, determining and order relation between every pair object-operation. Intuitively, the more user-permission strength, the more objects and operations links the permission. The multivalued user-permission relations allow to describe a user progression in the system. User-role relations are dynamic and allow to specify the membership level of users within roles. An increasing user-role magnitude will produce an increasing user-permission magnitude and will grant the user with more access privileges. Figure 3.2 shows a representation of polymorphic permissions.

Under this interpretation of continuous access, polymorphic permissions can be implemented through conditions in the access control policies, allowing to define the minimum access level that users must have to execute every action over every resource.

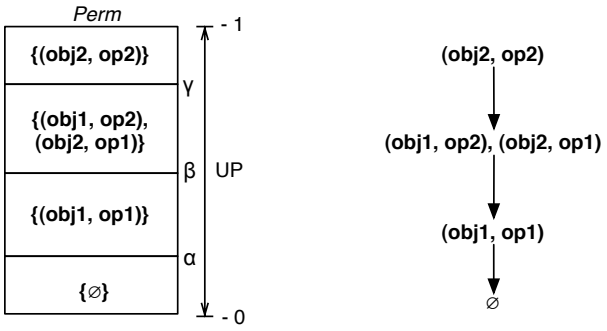

Figure 3.2: The user-permission strength determines the objects and operations related by the permission. The more permission strength (UP), the more objects and operations relates the permission. In this figure, an user-permission strength in the range $[0, \alpha)$ makes the permission to relate no objects and operations. A UP strength in the range $[\alpha, \beta)$ makes the permission to relate the $object_1$ with the $operation_1$ and so on.

In this case, users apply access requests and the decision point must determine if the access must be permitted or not.

Thresholded plain permissions

In the environments where RBAC applies, accesses are not seen under a continuous interpretation and permissions are plain. In order to guarantee the compatibility with RBAC, in these scenarios, FRBAC must issue binary access decisions and the access level must be expressed in terms of permit/deny, where 0 does not allow the access and 1 allows it. As a first approximation, a threshold can determine the minimum access degree that enables the access. Conditions in the access control policies can be used to determine the minimum access level that enables the execution of the permission. Again, users apply access requests and the decision point must determine if the access must be permitted or not.

Thresholded plain permissions are a particular case of polymorphic permissions, where the objects and operations related by the permission are placed above a unique

threshold. Figure 3.3 shows a representation.

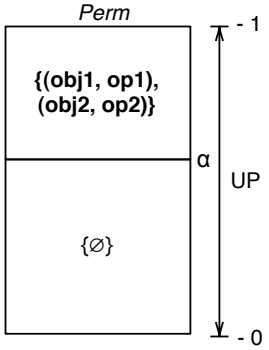

Figure 3.3: The user-permission strength determines the objects and operations related by the permission, placed over a unique threshold (α).

3.1.2 Contributions

Here are summarized the contributions of FRBAC to the research on access control:

- **Parametrized assignments**
  FRBAC enables the parametrization of user-role and role-permission assignments. Assignments in FRBAC go beyond the simple fact that a user or a permission is assigned to a role. User trustworthiness, user seniority, risk and uncertainty, are just few examples of semantics underlaying the assignments.

- **Access level**
  FRBAC proposes a new understanding of accesses. A novel decision mechanism states the access level in the range $[0, 1]$ that a given user has over a given resource through a given operation. Access level can be used to accommodate continuous accesses and polymorphic permissions.

- **Expressivity**
  In RBAC, a "role explosion" can result in thousands of separate roles being fashioned for different collection of permissions [22] when dealing with underlaying

semantics in the user-role assignment, such as user seniority. Multivalued user-role and role-permission assignments may help on the reduction of the number of roles, avoiding the need of role splitting. Polymorphic permissions keep tidied the access control policies, and may reduce the number of permissions and assignments in the access control policy. The reduction of roles, permissions and assignments results in a easier policy definition, thus preventing errors in this process.

- **More fine-grained RBAC policies**
  In RBAC, the minimum change in an access control policy is a user-role assignment or a role-permission assignment. Both represent a big modification on the privileges of users. The multivalued assignments of FRBAC benefit RBAC with more flexible access control policies. It eases, for instance, the definition of context-aware access control policies.

3.1.3 Applicability of FRBAC

Here are briefly described some application scenarios of FRBAC:

- **Data lying in databases**
  Data lying in databases is a queering mechanism that alters, to the end users, the information retrieved from the database in order to preserve some security requirements [39]. A censor module is in charge to distort the query responses adding a degree of noise. The noise degree attached to every response is variable and depends on the user's credentials or the user's history.

  FRBAC can easily accommodate an RBAC-based data lying scheme. The user-role relation strength can represent useful authorization-relevant semantics such as user's trustworthiness, user's seniority, user's need-to-know, or any other application-dependent information, which can be considered useful at authorization time. The role-permission relation strength must be coherent with

the user-role relation in order to enable their composition. Finally, the user-permission strength is interpreted as the access level that every user has over the database, and it is used in the censor module to enforce the execution of the query.

The censor module acts as the enforcement point of the application, and provides a continuous vision on the access to the database. A user with almost no privileges will be able to query the database but will not be able to obtain useful information because of the huge amount of noise attached to the response. A user with high privileges will be able to query the database and obtain low noise ratios in the responses.

- **Quality of service**

  Quality of service (QoS) aims to balance the resources put on serving every user in a system in order to enable certain users and applications to get better service than others at a higher cost [13, 16].

  FRBAC can accommodate an access control QoS-aware scheme. The user-role assignment may represent the premium degree of every user. In the same manner, the role-permission assignment may represent the premium degree of every role. The composition of both, the user-role and role-permission assignments represents the access level that every user has over every permission. This access level will lately determine the balancing of the resources put on serving every user.

  Scheduling the resources put on serving every user represents a form of continuous access when the scheduling is based on user prioritization. The more user-permission strength, the more resources put on serving the user and, thus, better quality of service.

- **Vague roles**

Roles represent in RBAC a well defined characterization of users in the organization chart. While there are roles that accept a crisp membership degree (like *doctor*, *nurse*, *surgeon*) there are roles vague in nature. Imagine the following role set: *child*, *teenager* and *adult*. Since the frontier between childhood, adolescence and adulthood may not be clear, and may vary form one person to another, a crisp characterization of users may not be expressive enough for the access control system.

The multivalued user-role assignments of FRBAC allows the description of vague roles. The user-role assignment strength can represent the degree in which users belong to roles, allowing a natural membership evolution from low to high membership degree, and then back to low.

The concept of vague roles fits well with the notion of polymorphic permissions. The natural evolution of the user-role membership degree would lead users to gain access power as they gain membership degree, allowing them to execute more actions over more resources. The loss of membership degree would lead users to loose access power.

- **Execution scope**

  In RBAC, permissions are defined as sets of pairs *object-operation*, meaning that the permission enables the execution of the given *operation* over the given *object*. However, objects may be uncountable or may not have an unique identity on the system. Imagine the case of a permission that enables the user to transfer money or issue invitations to an event. How many money or invitations can the user transfer?

  The parametrized user-permission assignments of FRBAC can be used to determine the degree in which users can access objects. A user-permission strength of 0 means the minimum access level to the object, while a user-permission of 1 means the maximum access degree. The permission *send_invitations*, would allow the user to issue a different number of invitations depending on

the user-permission strength. The variable execution avast represents a form of continuous access itself.

- **Risk-based access control**:

  In general, access control can be understood as a mechanisms used to manage risk, i.e., to balance the information needs of the users with the need of the organization to protect its sensitive information [8]. FRBAC can be used as the basis of a risk-based access control, where risk involving every access is related with the operation itself, the object of the operation and the initiating user. The execution is permitted if the involving risk is low enough.

  FRBAC allows to easily accommodate an RBAC risk-based access control scheme. User-role assignments may represent the risk involving the fact that a user plays a role. Risk can represent the user's trustworthiness based on the user's history. Similarly, role-permissions assignments may represent the risk involving every assignment. The composition of user-role and role-permissions assignments determines the user-permission assignment risk.

  Once the risk involving every user-permission assignment is known, the enforcement point of the application can determine whether to permit or deny the execution of a permission. Moreover, risk mitigation measures can be taken with the execution of a permission. Risk mitigation measures can be understood as a form of continuous access, where the strength of the executions are tuned to adapt the risk to a level that the system is willing to tolerate.

- **Trust-based access control**

  Trust-based access control is closely related with risk-based access control. In fact, trust and risk are closely related concepts. Trust is unnecessary unless there is something at risk [12]. In a pure trust-based access control scheme, the access level of every user is determined by the user trustworthiness. Intuitively, the more user trustworthiness, the more access level the user has. Access level is a mechanism to balance risk. A high access level represents high risk on

damaging the system. Thus, high access levels are only allowed to trusted users.

The multivalued nature of the assignments of FRBAC can easily represent trust-based relations. User-role relations may represent the trust degree of a given user playing a given role. Role-permission relations may be binary or represent the risk involving the assignment. The composition of the user-permission relation represents the risk involving every assignment.

The enforcement point of the application must evaluate if the risk involving every request is low enough to permit the access. Depending on the application, the access degree may be adapted to the trust involving the request. If actions are not seen under a continuous interpretation, access decision will be formulated in terms of permit/deny.

- **Progressive learning**

  When a user faces a new system, unknowing the system may cause frustration [25] to the user and may suppose a security threat to the system itself. A good training on the system's usage may help to dramatically reduce accidents and reduce the user frustration. Progressive abilities acquisition can be used as a learning method through a positive feedback cycle: users continually grow in power, allowing them to overcome more difficult challenges and gain even more power.

  The user-role relations of FRBAC can be used to determine the user progression within a role. The more a user belongs to a role, the more privileges the user obtain. Critical permissions are given once the user knows the system well. Tuning the assignments, the learning curve can be adapted for every user, every role or every permission. The same principle of progressive abilities acquisition can be adapted to progressive abilities loss. Progressive abilities loss may help on the process of a user leaving a system. It may prevent deliberate misuse of the system of users leaving an organization, for example.

- **Uncertain authentication information**

  In some environments, the fact that a user is assigned to a role is based on uncertain information. This phenomenon can be observed in the Aware Home Project [30], where the information available from sensors in the home should be used to automatically infer the user's security-relevant attributes (e.g., identity, role or location.). Many such sensors can establish the security-relevant attributes of a subject with only a partial level of certainty, or confidence level. It can be generalized to biometric-based authentication. Another field with intrinsic vague authorization-relevant information is the multi-domain environment under an attribute conversion based interoperability scheme. In these scenarios, user's credentials within their origin domain are converted to credentials of the target domain, thus foreign users may be treated as local ones. Imprecision arises from the impossibility to find absolute similarity on the credentials of the different domains but similarity to some degree.

  The FRBAC model can naturally accommodate the certainty of a user belonging to a role through the user-role assignment strength. The imprecision level will be propagated to the user-permission relation. This imprecision must be taken into account at the decision time in order to determine the access degree.

  The imprecision degree can be propagated through the user-permission relation to the access decision. The access decision can be formulated in terms of access level if the action being requested has a continuous meaning. Otherwise, the access decision can be binary, thresholding the imprecision degree that the system is willing to tolerate.

- **Flexibility through intra-domain role similarity**

  In RBAC, permissions enable the execution of certain actions over certain resources. A user acquires a permission only if the permission is assigned to one of the roles that the user plays. The similarity between different roles can be

used to flexibilize an access control system, enabling users to obtain permissions assigned to roles similar than the roles they play. Users may acquire the permissions assigned to the roles they play and, in less degree, the permissions assigned to those roles which are similar to the roles assigned to the users.

FRBAC enables the definition of role inheritance though a fuzzy relation, named RH. This fuzzy relation can be composed with the user-role relation in order to determine user-role assignments by virtue of the role inheritance. The role inheritance is described by a magnitude in the range $[0, 1]$ which semantics can represent the similarity between roles. In this manner, users can inherit roles and acquire the related permissions. The user-permission strength takes into account the role inheritance strength. The less role inheritance strength will result in less user-permission strength, and thus, less access level.

- **Context awareness in RBAC**

  The very definition of RBAC does not describe any form of context awareness. Some proposals aim to condition the user-role, role-permissions assignments, or role activation to the environment state [20, 10, 41, 5, 23]. However, conditioning the user-role, the role-permission assignments, or the role activation, may lead users to experience big "stairstep" jumps in permissions.

  FRBAC helps on a smooth context adaption through the multivalued user-role and role-permission assignments. Rather than completely assign or deassign users and permissions from roles, FRBAC allows a fine-tuning on the assignments to the context state. Thus, little context modifications will produce little authorization changes. It is noteworthily to point out that coherence between user-role and role-permission assignments must be respected in order to allow their composition. The context must be sensed and crawled to reduce all the possible variables to parametrized semantics in the user-role and role-permission assignments. Once composed the user-permission relation, the strength of every assignment will be taken into account to determine the access degree.

The definition of polymorphic permissions and the access level could also be related to the context state.

- **Others**
  In general, multivalued user-role and role-permission relations can be used to represent any application-specific semantics that can condition the assignments. History-based access control, location-based access control, credit-based access control, or qualification-based access control are just few more examples of applicability of FRBAC. Many other apply.

3.2 Attribute conversion

The growth and recent advances in distributed systems and computer networks enable existing systems and services to interact in order to provide new and improved applications. With the interoperation comes the challenge of ensuring a consistent interpretation of the access control across the heterogeneous domains and shared resources. Previous research considered the problem of access control interoperation from different points of view [2, 4, 19, 32], however most of the proposals assume the redefinition of the access control policies of every existing system [36, 35], which will not be practical in most of cases.

Imagine an scenario with two independent administrative domains A, and B. When a user from domain A needs to access a resource owned by domain B, the first problem that arises is that the attributes of the user in the domain A are not understandable in the domain B. To enable the authorization of the user, her attributes, understandable in the domain A, must be converted to attributes in the domain B. Intuitively, the role *sales manager* from domain A can be converted to the role *marketing manager* from the domain B. Thus, the user can be submitted to the local access control policies in the domain B which regulates the access to the desired resource. This approach avoids the need to redefine the local access control

policies of every participating domain.

In the general case, it will not be realistic to find total equivalence between attributes of heterogeneous domains. On the contrary, we propose to measure the similarity between attributes and take it into account in the conversion process. In this manner, it can be defined that the role *sales manager* from domain A is 90% similar to the role *marketing manager* defined in the domain B. We propose attribute conversion policies as fuzzy relations that determine the similitude between the attributes of two domains. It will be lately determined whether the similarity is high enough to issue the local attribute in the target domain from the original one.

The generation of conversion policies is a previous step before the interoperation itself. The security administrators of every pair of domains must establish the similitude between the attributes of one domain to the other. The similitude arises from the study of the semantics of every attribute. It is noteworthily to point out that conversion policies are not symmetric since converting the attributes from the domain A to the domain B does not necessarily enable the conversion between attributes from the domain B to attributes of the domain A. The target domain takes the responsibility in the conversion. Consider for example the case where A is the library of a town, and B is the nuclear power plant of the same town. A may allow the conversion of attributes from B which may allow employees of B to borrow books from A, but B will not allow conversion of attributes from A.

The generation of attribute conversion policies between every pair of domains in the interoperation scenario may not be practical for scalability issues. A scenario with n domains needs $n^2 - n$ attribute conversion policies in order to enable the conversion of attributes between any two domains. As the number of domains grows, the number of required conversion policies grows exponentially. Our approach is scalable in the sense that it is not necessary to a priory specify every pairwise policy interoperation relationship, rather, where obvious interpretations exist then attribute relationships are defined, while other relationships are inferred by transitivity. If attribute a is somewhat similar to attribute b and attribute b has similarity with attribute c. By

transitivity, attribute a and attribute c are somewhat similar. Transitivity is achieved by aggregating the attribute conversion policies. The aggregating process forwards the similitude along the aggregation chain.

3.2.1 Evolution

Since the contribution "Flexible secure inter-domain interoperability through attribute conversion" was published, the research has been kept active in this area. In the following we introduce an unpublished evolution of the mechanism which guarantees the privacy on the attribute conversion policies. In the following we use a similar notation than the described in the published contribution.

We differentiate between two types of conversion networks:

- **Public conversion networks**: Public conversion networks assume that all the conversion policies are known by all the domains in the scenario. When an attribute conversion have to be carried out between two domains with no attribute conversion policy between them, the target domain of the conversion gets the appropriate conversion policies whose composition enables the conversion of attributes.

- **Private conversion networks**: Private conversion networks are based on two privacy assumptions. The existence of a relation which allows the conversion between two domains is only known by such domains, which are called *neighbours*; and the actual conversion function or relation is only known by the target domain. That is, A and B know the existence of C_{AB}, but C_{AB} is only known by B. Private conversion networks is unpublished research.

Private conversion networks

In private networks we use a collaborative approach to convert attributes. The conversion is achieved by propagating intermediate compositions through the network.

As in public networks the goal is to end up with a relation from the origin domain A_0 to the target A_z. For that, we consider a conversion network as directed graph, where the set of vertexes is the set of domains and the directed arcs are the conversion relations. We denote the *out-neighbourhood* of a domain D as $N^+(D)$, comprising all domains reachable through an outgoing arc and the *in-neighbourhood* of a domain D as $N^-(D)$ with all the nodes connected through an ingoing arc. Figure 3.4 shows an example of a relation network.

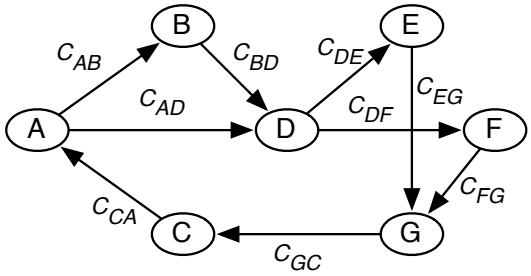

Figure 3.4: Relation network example.

Every domain in the conversion network collaborates by propagating messages containing a temporal relation R_i, the target domain A_z and a TTL (time-to-live). Normally, each domain composes the received relation with its corresponding conversion function to obtain a new temporal relation. The domain also decreases the TTL of the message after propagating it. When the TTL reaches 0 the message is discarded and no further propagated. The TTL of the message ensures that no message will be propagated forever in the network even in the presence of loops. Loops can also be avoided completely by including a list of the nodes in the message.

The attribute conversion in private networks is achieved through the process described in Algorithm 1. It takes a subset of attributes in the origin domain ($P \in A_0$) as an argument and provides a final conversion function as the relation $C_{PA_z} : P \times A_z \rightarrow [0, 1]$. For a given user u, we will take $P = u(A_0)$, but depending on the scenario one could consider a more generic set $P \subseteq u(A_0)$.

As it can be seen an important issue in the protocol is the *timeout* T that A_z

waits in order to produce the final relation. This timeout attempts to ensure that A_z receives all possible intermediate relations for all possible paths from A_0. Since A_z does not know the topology of the network, there is no way for A_z to know how many paths are there, and thus, how many intermediate relations should be received. This makes the whole procedure non-deterministic, but more flexible and efficient from a practical point of view. The timeout is set by each domain depending on the perception of the network longitude and of course can be tuned if required.

Algorithm 1: Attribute conversion in private conversion networks.

Input: Origin domain A_0, target domain A_z, a set of attributes $P \subseteq A_0$

Output: $C_{PA_z} : A_0 \times A_z \rightarrow [0, 1]$

begin

  Domain A_0 creates a relation R_0 such that:

  $$R_0(x, y) \leftarrow \begin{cases} 1 & \text{if } x = y, \forall x, y \in P \\ 0 & \text{otherwise} \end{cases};$$

  Domain A_0 sends $\langle R_0, A_z, TTL \rangle$ to all its out-neighbours $N_G^+(A_0)$;

  foreach *domain* A_i *on receiving* $\langle R_{i-1}, A_z, TTL \rangle$ *from domain* $A_{i-1} \in N_G^-(A_i)$ **do**

    if $A_i \neq A_z$ **then**

      if $TTL = 0$ **then**

        Discard message;

      else

        A_i calculates $R_i \leftarrow R_{i-1} \circ C_{A_{i-1}A_i}$;

        A_i sends $\langle R_i, A_z, TTL - 1 \rangle$ to all its out-neighbours $N_G^+(A_i)$;

      end

    else

      A_z calculates $R_z \leftarrow R_{i-1} \circ C_{A_{i-1}A_z}$;

      A_z saves R_z forming a list with all relation received and rooted at A_0 as $\{R_z^1, R_z^2, \ldots\}$;

      A_z waits timeout T;

      A_z calculates $C_{PA_z} \leftarrow \bigcup_i R_z^i$;

      return C_{PA_z}

    end

  end

end

3.2.2 Contributions

Here are summarized the contributions of the attribute conversion mechanism to the research on the interoperation of authorizations systems:

- **Realistic: based on similarity**

  The concept of attribute conversion has been previously studied by some authors [2, 27, 40, 28, 29]. However, the previous definitions of attribute conversion assume that there exists an absolute similarity relation between the attributes of the different domains. In an heterogeneous scenario this assumption may not be true. The proposed mechanism assumes that in the general case it may not be possible to find absolute similarity relations and, thus, considers the similarity degree in all the conversions.

- **Scalable**

  A transversal hitch on interoperation, in all of its forms, is scalability. In attribute conversion based interoperability, the number of required conversion policies in the scenario is exponential to the number of interoperating domains. In an scenario with n domains, $n^2 - n$ interoperation policies are needed in order to enable full connectivity. Our approach is scalable in the sense that it is not necessary to a priory specify every pairwise policy interoperation relationship, rather, where obvious interpretations exist then attribute relationships are defined, while other relationships are inferred by transitivity, dramatically reducing the number of conversion policies to n conversion policies in the best case (circle-like topology).

3.2.3 Applicability

Although the proposed mechanism can be used in any interoperation scenario, here we briefly describe some scenarios that make our scheme most appropriate than the rest.

- **Quick collaboration**

  Attribute conversion is one of the simplest forms of collaboration which minimizes the pre-interoperation tasks. However, in an scenario with several domains, the time involved on the generation of conversion policies may be too high. The proposed conversion mechanism helps, by transitivity, on the reduction of the required conversion policies in the scenario, thus reducing the time involved on setting the scenario.

- **Massive collaboration**

  Our scheme reduces the number of interoperation policies in a massive collaboration scenario through transitivity. The proposed mechanism enables the conversion of attributes between any two domains through n conversion policies in an scenario with n domains. This lowest boundary is achieved through a circle-like topology. Without transitivity in the conversion process, the number of required conversion policies is $n^2 - n$ in an scenario with n domains, which is unmanageable.

- **Dynamic collaboration scenarios**

  Our scheme can be used in dynamic collaboration scenarios where domains can join and leave the scenario frequently. The attribute conversion mechanism avoids the need of the generation of global access control policy every time that a domains joins or leaves the scenario. The transitivity of attribute conversion policies reduces the effort of the generation of attribute conversion policies that enables new domains to join the collaboration in a quick way.

- **Adaptive collaboration: context awareness**

  The multivalued nature of the attribute conversion policies based on similarity enables a fine-grained context adaption of the collaboration. Similarity degrees can be tuned at any time during the collaboration. The number domains in the scenario, their internal organization, trust relations between domains, and

external risk threats are just few examples of factors that adaptive attribute conversion policies may be aware of.

- **Meta collaboration**
  Meta collaboration refers to collaboration between previously set interoperation scenarios. Imagine that more than one collaboration scenario involving several domains, come together to share resources. By transitivity, our collaboration mechanism enables the definition of bridge attribute conversion policies between the different scenarios to enable the meta-interoperation.

3.3 Attribute conversion in FRBAC domains

The proposed attribute conversion mechanism enables the conversion of attributes between heterogeneous access control models. However, the attribute conversion mechanism and FRBAC together enable a new understanding of imprecision management.

The attribute conversion mechanism is, in fact, an automatic attribute assigner. Depending on the user's attributes in the user's home domain, the attribute conversion mechanism determines the user's attributes in the rest of the interoperating domains. Attribute conversion policies determine the similitude between attributes of the different domains. In the general case, similitude relations between attributes are not absolute. The similarity degree between attributes represents an imprecision or error measure in the conversion process. The less similitude between two attributes, the more imprecision in the conversion.

When the attribute conversion mechanism deals with no imprecision-tolerant access control models, such as RBAC, the mechanism must determine whether to enable the conversion of two attributes depending on the similarity between them. With this propose, every interoperating domain states the maximum imprecision degree that it is willing to tolerate. In other words, a threshold determines the minimum similarity between two attributes which enables the conversion of one attribute to the other. If

the similarity between two attributes is high enough, the conversion can be carried out and, thus, the user will be assigned with local attributes in the target domain. This last step on the attribute conversion issues absolute user-attribute assignments in spite of the remaining imprecision of the conversion process. Figure 3.5 represents the attribute conversion process.

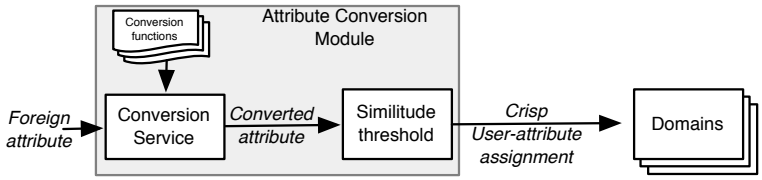

Figure 3.5: Attribute conversion process.

FRBAC deals with parametrized user-role assignments, and propagates this imprecision to the access decision. Intuitively, the more strength in the user-role assignment, the more access degree the user has over the permissions assigned to the role. The concept of access level fits well with the imprecision on the conversion process. In a collaboration scenario involving FRBAC domains, rather than thresholding the maximum imprecision degree that every domain is willing to tolerate, the user-role assignments by virtue of the collaboration may capture the imprecision of the conversion process in the user-role assignment strength. In other words, the parametrized UA relation will reflect the imprecision in the conversion process. The imprecise user-role assignments will lately determine the access level that every user has over every permission in every domain. A low user-role strength means high imprecision in the conversion process and, thus, low access level. Figure 3.6 represents the attribute conversion process in FRBAC domains.

3.3.1 Attribute conversion and parametrized assignments

FRBAC enables the description of parametrized user-role assignments through the fuzzy relation UA. The attribute conversion mechanism must take into account the

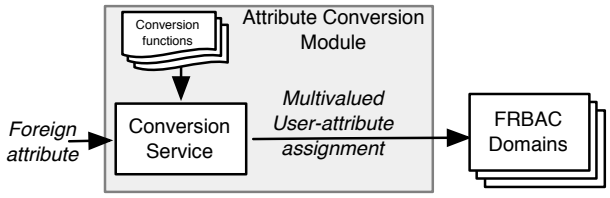

Figure 3.6: Attribute conversion process in FRBAC domains.

parametrized user-role assignments in the target domain in order to determine the equivalent user-role assignments in the rest of domains. Imagine that a given user owns $role_1$ in her origin domain, and an attribute conversion policy specifies that $role_1$ is 0.9 similar to $role_2$ defined in other domain. It is clear that if the user owns $role_1$ with a magnitude of 0.1, she cannot own the $role_2$ under a magnitude of 0.9.

We call UA_X^X the user-role assignment relation of users of the domain X in the domain X. C_{XY} represents the conversion policy between attributes form the domain X to attributes in the domain Y. UA_Y^X represents the user-role assignment relating users from domain X with attributes in the domain Y. The composing operand $\circ$ stands for the standard *max-min* composition of two fuzzy relations. Let $R1 : X \times Y \rightarrow [0, 1]$ be a fuzzy relation defined as collection of items of the form $((x, y), \mu_{R1}(x, y))$ where $x \in X$, $y \in Y$, and $\mu_{R1}(x, y) \in [0, 1]$. Let $R2 : Y \times Z \rightarrow [0, 1]$ be a fuzzy relation. The *max-min* composition $R1 \circ R2 : X \times Z \rightarrow [0, 1]$ is defined as follows:

$$R1 \circ R2 = \{((x, z), \max_y(\min(\mu_{R1}(x, y), \mu_{R2}(y, z))))|x \in X, y \in Y, z \in Z\}$$

User-role assignments of a given domain (X) can be translated to user-role assignments of another domain (Y) in the scenario through the composition of the user-role relation and the conversion policy (UA_Y^X):

- $UA_Y^X = UA_X^X \circ C_{XY}$

In the presence of a role hierarchical relation (RH_X) in the origin domain (X):

- $UA_Y^X = UA_X^X \circ RH_X \circ C_{XY}$

In the presence of a role hierarchical relation (RH_Y) in the target domain (Y):

- $UA_Y^X = UA_X^X \circ C_{XY} \circ RH_Y$

In the presence of role hierarchical relation in the origin and the target domain:

- $UA_Y^X = UA_X^X \circ RH_X \circ C_{XY} \circ RH_Y$

The conversion departs from a user-role relation of the type $USERS \times ROLES \rightarrow [0, 1]$ which composed with an attribute conversion policy of the type $ROLES \times ROLES \rightarrow [0, 1]$ outputs a user-role relation of the type $USERS \times ROLES \rightarrow [0, 1]$. The output relation determines the user-role assignments from users of an origin domain with attributes of a target domain. However, the interpretation that every domain gives to the user-role assignments may be different in the scenario and the attribute conversion process must be aware of them.

Imagine that $user1_A$ owns the $role1_A$ in the domain A under a magnitude of 0.5. The domain A interprets that the parametrized assignments represents user seniority. Imagine now that $role1_A$ is totally equivalent to the $role1_B$ in the domain B. It is clear that if $user_1$ owns the $role1_A$ under a magnitude of 0.5 in the domain A, by virtue of the equivalence relation, $user1_A$ owns under a magnitude of 0.5 the $role1_B$ in the domain B. The problem might arise from the interpretation that domain A and B makes of the parametrized assignments.

While domain A may interpret that parametrized user-role assignments represents user seniority, domain B may interpret that parametrized user-role assignments represents the current distance of the user with respect to the central building of the enterprise. It is clear that the user-role assignment strength in the origin domain cannot be always taken into account to determine the user-role assignment strength in the target domain. As a first approximation, only if the origin and the target domain interpret in a similar way the user-role assignments, the user-role assignment strength in the origin domain can be used to determine the user-role assignment strength in the target domain. The interoperation between FRBAC domains that do not interpret the user-role assignments in a compatible way is still an open research issue.

Example

Imagine two FRBAC domains involved in a collaboration agreement: domain A and domain B. Both domains make a similar interpretation of the parametrized user-role assignments. The access control policy of A defines the roles $r1_A, r2_A, r3_A$. The access control policy of domain B defines the following roles: $r1_B, r2_B$. The user-role assignments in the domain A (UA_A^A) are defined in Table 3.1.

	$r1_A$	$r2_A$	$r3_A$
$user1_A$	0.9	0	0

Table 3.1: User-role assignment in the domain A.

The security administrators of domain A and B have agreed in the similarity-based attribute conversion policy (C_{AB}) shown in Table 3.2.

	$r1_B$	$r2_B$
$r1_A$	1	0.5
$r2_A$	0.2	0
$r3_A$	0	0.3

Table 3.2: C_{AB} Attribute conversion policies.

The user-role assignments between users from domain A and roles in the domain B (UA_B^A) is given by the *max-min* composition of the user-role assignments in the domain A (UA_A^A) and the attribute conversion policy between the domains A and B (C_{AB}). Table 3.3 represents UA_B^A.

	$r1_B$	$r2_B$
$user1_A$	0.9	0.5

Table 3.3: $UA_B^A = UA_A^A \circ C_{AB}$.

Chapter 4

Conclusions

This thesis bets for a new understanding of access control, where the access decisions are not issued in the form permit/deny but the decisions state the access level that users have over objects through operations. In this thesis FRBAC has been proposed. FRBAC is a generalization of RBAC which issues access control decisions in terms of access level. The concept of access level represents a first step towards a new understanding of access control where the access control models are not limited to permit and deny the accesses but to determine and enforce the access degree of every access request.

The concept of access level is closely related with the parametrizing semantics of the assignments in FRBAC. FRBAC allows to parametrize the user-role and role-permission assignments depending on semantics like user trustworthiness or uncertainty involving the identification process. The underlaying semantics on the assignments can be taken into account along the authorization process in order to determine the access level that users have over resources.

In this thesis, it has also been proposed the concept of polymorphic permissions, which represents a new understanding of the permissions described in a system. Polymorphic permissions aims to condition to the access level the actions that users can

execute over resources. Polymorphic permissions can be used to describe the progression that users can experience within a system as their access level is increased, representing a different understanding of the concept of roles than the described in RBAC. Now, roles does not only describe the static set of permissions related with every user but roles imposes limits in the abilities acquisition and enhancing that users can experience in the system.

Finally, the multivalued user-role and role-permission assignments in FRBAC enables the description of fine-grained RBAC-like policies, where belonging to a role does not necessarily mean acquiring the whole set of permissions assigned to the role, allowing users to progress in the roles they play.

This thesis also proposes an attribute-conversion mechanism that enables the interoperation between different domains with heterogeneous access control models. The mechanism manages the intrinsic imprecision in the similarity-based attribute-conversion process, issuing parametrized user-attribute assignments. Parametrized user-attribute assignments can be binarized to enable the interoperation between no parametrization-tolerant access control models, like RBAC. However, through the parametrized user-role assignments, FRBAC provides a new way to manage the intrinsic imprecision involving an attribute conversion process forwarding it, through the concept of access level, towards the access decision.

Through the similarity-based conversion policies, the attribute conversion mechanism provides a realistic and generic attribute-level interoperation between domains. The transitiveness of the conversion process benefits the scalability of the system dramatically reducing the required attribute conversion policies in the scenario.

4.1 Future research lines

At this end stage of the thesis, many future research lines arise. In the following we describe some of them.

- **XACML implementation of FRBAC**

It has been shown the description and applicability of FRBAC. However, it might be interesting to propose an XACML [31] extension implementing FRBAC.

- **Context awareness in FRBAC**
  Despite context awareness in FRBAC has been introduced in Section 3.1.3, it is still an open issue at this moment. The user-role and role-permission assignments can be conditioned to the context state. However, it is necessary a mechanism to capture the contextual information and reduce it to user-role and role-permission assignments, respecting the coherence between them in order to enable their composition. Furthermore, the definition of polymorphic permissions and the notion of access level can be also subjected to the context state.

- **Different aggregation methods for the user-role and role permissions assignments in FRBAC**
  User-permission assignments arises from the standard *max-min* composition of the user-role and the role-permission relations. Although we use the *maximum* operand as the union and the *minimum* as the intersection of fuzzy sets, other *t-conorm* and *t-norm* operands could be used respectively, giving up also to another relation composing operands [21].

- **Different defuzzification methods in FRBAC**
  FRBAC deals with actions that provide a continuous interpretation of the access. Fractionality strongly depends on the application. However, there are actions with no possible continuous interpretation. When dealing with this actions, FRBAC defuzzificates the access level in order to issue permit/deny decisions. In its present form, a security threshold determines the minimum access level that enables the execution of the action. More sophisticated mechanisms can be described.

- **Multi-dimensional parametrized assignments in FRBAC**
  FRBAC enables the parametrization of the user-role and role-permission assignments. Risk, trust, or uncertainty are just few examples of the semantics underlaying the assignments. However, by the own nature of the user-role and role-permission assignments, they can be parametrized in one dimension. It would be interesting to parametrize the assignments in a multidimensional way and study the impact on the access level of each semantics.

- **Study the interoperation between FRBAC domains with heterogeneous semantics in the user-role assignments**
  The interpretation that a given domain gives to parametrized user-role assignments may be different than the interpretation that gives another domain (See Section 3.3.1). It might be interesting to study the interoperation issues between domains with different interpretation in the user-role assignments.

- **Algorithms to search for (optimal) re-configuration**
  Suppose that a converted attribute relation is below a conversion threshold, then it would be interesting to determine the set of changes that could be made to the conversion graph that would result in the desired threshold. There might be an interesting optimization aspect to this, such as what's set of changes that would result in the smallest, in some sense, impact of the individual policies.

- **Many-to-* conversions**
  The attribute conversion policies enable the conversion of attributes in a one-to-one and one-to-many form. It would be interesting to enable the conversion of attributes in a many-to-one and many-to-many way, respecting the transitivity of the conversion process.

Bibliography

[1] R. J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 1st ed. New York, NY, USA: John Wiley & Sons, Inc., 2001.

[2] J. Bacon, K. Moody, and W. Yao, "Access control and trust in the use of widely distributed services," in *Proceedings of IFIP/ACM International Conference on Distributed Systems Platforms*, ser. Lecture Notes in Computer Science, vol. 2218. Springer, 2001, pp. 295–310. [Online]. Available: http://portal.acm.org/citation.cfm?id=646591.697775

[3] D. E. Bell and L. J. LaPadula, "Secure Computer Systems: Mathematical Foundations," MITRE Corporation, Tech. Rep., 1973.

[4] P. Belsis, S. Gritzalis, and S. Katsikas, "A scalable security architecture enabling coalition formation between autonomous domains," in *Proceedings of 5th IEEE International Symposium on Signal Processing and Information Technology.* IEEE, Dec. 2005, pp. 560–565.

[5] E. Bertino, B. Catania, M. L. Damiani, and P. Perlasca, "Geo-rbac: a spatially aware rbac," in *Proceedings of the tenth ACM symposium on Access control models and technologies*, ser. SACMAT '05. New York, NY, USA: ACM, 2005, pp. 29–37. [Online]. Available: http://doi.acm.org/10.1145/1063979.1063985

[6] B. Blakley, "The emperor's old armor," in *Proceedings of the 1996 workshop on New security paradigms*. ACM Press, 1996, pp. 2–16. [Online]. Available: http://doi.acm.org/10.1145/304851.304855

[7] M. Blaze, J. Feigenbaum, J. Ioannidis, and A. Keromytis, "Rfc 2704-the keynote trust-management system version 2."

[8] P.-C. Cheng, P. Rohatgi, C. Keser, P. Karger, G. Wagner, and A. Reninger, "Fuzzy multi-level security: An experiment on quantified risk-adaptive access control," in *Security and Privacy, 2007. SP '07. IEEE Symposium on*, may 2007, pp. 222 –230.

[9] P.-C. Cheng, P. Rohatgi, C. Keser, P. A. Karger, G. M. Wagner, and A. S. Reninger, "Fuzzy multi-level security: An experiment on quantified risk-adaptive access control," in *Proceedings of the 2007 IEEE Symposium on Security and Privacy*, ser. SP '07. Washington, DC, USA: IEEE Computer Society, 2007, pp. 222–230. [Online]. Available: http://dx.doi.org/10.1109/SP.2007.21

[10] M. J. Covington, W. Long, S. Srinivasan, A. K. Dev, M. Ahamad, and G. D. Abowd, "Securing context-aware applications using environment roles," in *SACMAT '01: Proceedings of the sixth ACM symposium on Access control models and technologies*. New York, NY, USA: ACM, 2001, pp. 10–20.

[11] N. Damianou, N. Dulay, E. Lupu, and M. Sloman, "The ponder policy specification language," in *Proceedings of the International Workshop on Policies for Distributed Systems and Networks*, ser. POLICY '01. London, UK: Springer-Verlag, 2001, pp. 18–38. [Online]. Available: http://portal.acm.org/citation.cfm?id=646962.712108

[12] N. Dimmock, J. Bacon, D. Ingram, and K. Moody, "Risk models for trust-based access control(tbac)," in *iTrust*, 2005, pp. 364–371.

[13] C. Dovrolis and P. Ramanathan, "A case for relative differentiated services and the proportional differentiation model," *Network, IEEE*, vol. 13, no. 5, pp. 26 –34, sep/oct 1999.

[14] C. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas, and T. Ylonen, "Rfc 2693: Spki certi cate theory," 1999.

[15] D. F. Ferraiolo, R. S. Sandhu, S. I. Gavrila, D. R. Kuhn, and R. Chandramouli, "Proposed NIST standard for role-based access control," *ACM Transactions on Information Systems Security*, vol. 4, no. 3, pp. 224–274, 2001.

[16] S. N. Foley, "Supporting imprecise delegation in KeyNote," in *Proceedings of International Security Protocols Workshop*, ser. Lecture Notes in Computer Science, vol. 2845. Springer, 2002, pp. 179–188.

[17] W. Graf, "Territorialism in deer," *Journal of Mammalogy*, vol. 37, no. 2, pp. 165–170, 1956.

[18] M. A. Harrison, W. L. Ruzzo, and J. D. Ullman, "Protection in operating systems," *Commun. ACM*, vol. 19, pp. 461–471, August 1976. [Online]. Available: http://doi.acm.org/10.1145/360303.360333

[19] J. B. D. Joshi, R. Bhatti, E. Bertino, and A. Ghafoor, "Access-control language for multidomain environments," *IEEE Internet Computing*, vol. 8, no. 6, pp. 40–50, 2004.

[20] J. B. Joshi, E. Bertino, U. Latif, and A. Ghafoor, "A generalized temporal role-based access control model," *IEEE Transactions on Knowledge and Data Engineering*, vol. 17, no. 1, pp. 4–23, 2005.

[21] G. J. Klir and B. Yuan, *Fuzzy sets and fuzzy logic: theory and applications*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1995.

[22] D. R. Kuhn, E. J. Coyne, and T. R. Weil, "Adding attributes to role-based access control," *Computer*, vol. 43, no. 6, pp. 79 –81, june 2010.

[23] D. Kulkarni and A. Tripathi, "Context-aware role-based access control in pervasive computing systems," in *Proceedings of the 13th ACM symposium on Access control models and technologies*, ser. SACMAT '08. New York, NY, USA: ACM, 2008, pp. 113–122. [Online]. Available: http://doi.acm.org/10.1145/1377836.1377854

[24] B. W. Lampson, "Protection," *SIGOPS Oper. Syst. Rev.*, vol. 8, pp. 18–24, January 1974. [Online]. Available: http://doi.acm.org/10.1145/775265.775268

[25] J. Lazar, A. Jones, M. Hackley, and B. Shneiderman, "Severity and impact of computer user frustration: A comparison of student and workplace users," *Interacting with Computers*, vol. 18, no. 2, pp. 187 – 207, 2006. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0953543805000561

[26] H. Lockhart and B. Campbell, "Security Assertion Markup Language (SAML) V2.0 Technical Overview," Tech. Rep., mar 2008. [Online]. Available: http://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf

[27] G. López, O. Cánovas, and A. Gómez-Skarmeta, "Use of XACML policies for a network access control service," in *Proceedings of 4th International Workshop for Applied PKI*. IOS Press, Sep. 2005, pp. 111–122.

[28] G. López, O. Cánovas, A. F. Gómez-Skarmeta, S. Otenko, and D. W. Chadwick, "A heterogeneous network access service based on PERMIS and SAML," in *Proceedings of 2nd European PKI Workshop*, ser. Lecture Notes in Computer Science, vol. 3545. Springer, 2005, pp. 55–72.

[29] J. Luo, X. Ni, and J. Yong, "A trust degree based access control in grid environments," *Information Sciences*, vol. 179, no. 15, pp. 2618–2628, 2009.

[30] M. C. Matthew, M. J. Moyer, and M. Ahamad, "Generalized role-based access control for securing future applications," 2000.

[31] OASIS, "extensible access control markup language (xacml) version 2.0," OASIS Access Control TC, Tech. Rep., February 2005.

[32] L. Pearlman, C. Kesselman, V. Welch, I. Foster, and S. Tuecke, "The community authorization service: Status and future," in *Proceedings of Computing in High Energy Physics*. UCSD, 2003.

[33] D. Povey, "Optimistic security: a new access control paradigm," in *Proceedings of the 1999 workshop on New security paradigms*, ser. NSPW '99. New York, NY, USA: ACM, 2000, pp. 40–45. [Online]. Available: http://doi.acm.org/10.1145/335169.335188

[34] P. Samarati and S. de Vimercati, "Access control: Policies, models, and mechanisms," in *Foundations of Security Analysis and Design*, ser. Lecture Notes in Computer Science, R. Focardi and R. Gorrieri, Eds. Springer Berlin / Heidelberg, 2001, vol. 2171, pp. 137–196.

[35] B. Shafiq, J. Joshi, E. Bertino, and A. Ghafoor, "Optimal secure interoperation in a multidomain environment employing RBAC policies," CERIAS, Purdue University, Tech. Rep. 2003-24, 2003.

[36] ——, "Secure interoperation in a multidomain environment employing RBAC policies," *IEEE Transactions on Knowledge and Data Engineering*, vol. 17, no. 11, pp. 1557–1577, 2005.

[37] P. Vieira-Marques, S. Robles, J. Cucurull, R. Cruz-Correia, G. Navarro-Arribas, and R. Martí, "Secure integration of distributed medical data using mobile agents," *IEEE Intelligent Systems*, vol. 21, no. 6, November-December 2006.

[38] L. Wang, D. Wijesekera, and S. Jajodia, "A logic-based framework for attribute based access control," in *FMSE '04: Proceedings of the 2004 ACM workshop on Formal methods in security engineering*. New York, NY, USA: ACM, 2004, pp. 45–55.

[39] L. Wiese, "Keeping secrets in possibilistic knowledge bases with necessity-valued privacy policies," in *Computational intelligence for knowledge-based systems design, 13th international conference on Information processing and management of uncertainty*, ser. IPMU'10. Berlin, Heidelberg: Springer-Verlag, 2010, pp. 655–664. [Online]. Available: http://portal.acm.org/citation.cfm?id=1876326.1876406

[40] D. Wu, X. Chen, J. Lin, and M. Zhu, "Ontology-based RBAC specification for interoperation in distributed environment," in *Proceedings of 1st Asian Semantic Web Conferencer*, ser. Lecture Notes in Computer Science, vol. 4185. Springer, Sep. 2006, pp. 179–190.

[41] G. Zhang and M. Parashar, "Context-aware dynamic access control for pervasive applications," in *Proceedings of the Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2004), 2004 Western MultiConference (WMC)*, S. for Modeling and S. I. (SCS), Eds., Society for Modeling and Simulation International (SCS), January 2004.

Appendix A

"Fuzzy role-based access control"

```
@article{Martinez-Garcia:2011:FRA:1961710.1961854,
author = {Mart\'{\i}nez-Garc\'{\i}a, Carles and Navarro-Arribas, Guillermo
          and Borrell, Joan},
title = {Fuzzy Role-Based Access Control},
journal = {Inf. Process. Lett.},
issue_date = {April, 2011},
volume = {111},
issue = {10},
month = {April},
year = {2011},
issn = {0020-0190},
pages = {483--487},
numpages = {5},
url = {http://dx.doi.org/10.1016/j.ipl.2011.02.010},
doi = {http://dx.doi.org/10.1016/j.ipl.2011.02.010},
acmid = {1961854},
publisher = {Elsevier North-Holland, Inc.},
address = {Amsterdam, The Netherlands, The Netherlands},
keywords = {Databases, Role-Based Access Control,
           Safety/security in digital systems, Uncertainty},
}
```

Appendix B

"Intra-role progression in RBAC: An RPG-like access control scheme"

```
@INPROCEEDINGS{rpg-like,
author = {Mart\'{\i}nez-Garc\'{\i}a, Carles and Navarro-Arribas, Guillermo
          and Borrell, Joan},
title = {Intra-role progression in RBAC: An RPG-like access control scheme.},
note = {Submitted to 4th International Workshop on Autonomous and
        Spontaneous Security (SETOP)},
year = {2011},
pages = {},
month = {September}
}
```

Appendix C

"Flexible secure inter-domain interoperability through attribute conversion"

```
@article{Martinez-Garcia:2011:FSI:1988091.1988508,
author = {Mart\'{\i}nez-Garc\'{\i}a, Carles and Navarro-Arribas, Guillermo and
         Foley, Simon N. and Torra, Vicen\c{c} and Borrell, Joan},
title = {Flexible secure inter-domain interoperability through attribute conversion},
journal = {Inf. Sci.},
issue_date = {August, 2011},
volume = {181},
issue = {16},
month = {August},
year = {2011},
issn = {0020-0255},
pages = {3491--3507},
numpages = {17},
url = {http://dx.doi.org/10.1016/j.ins.2011.04.023},
doi = {http://dx.doi.org/10.1016/j.ins.2011.04.023},
acmid = {1988508},
publisher = {Elsevier Science Inc.},
address = {New York, NY, USA},
keywords = {Access control, Attribute conversion, Flexibility, Interoperability},
}
```

Appendix D

"An access control scheme for multi-agent systems over multi-domain environments"

```
@incollection {springerlink:10.1007/978-3-642-00487-2_43,
author = {Martínez-García, C. and Navarro-Arribas, G. and Borrell, J.
         and Martín-Campillo, A.},
affiliation = {Universitat Autònoma de Barcelona Dept. of Information
              and Communication Engineering},
title = {An Access Control Scheme for Multi-agent Systems over Multi-Domain
        Environments},
booktitle = {7th International Conference on Practical Applications of Agents
            and Multi-Agent Systems (PAAMS 2009)},
series = {Advances in Intelligent and Soft Computing},
editor = {Demazeau, Yves and Pavón, Juan and Corchado, Juan and Bajo, Javier},
publisher = {Springer Berlin / Heidelberg},
isbn = {978-3-642-00486-5},
keyword = {Books},
pages = {401-410},
volume = {55},
url = {http://dx.doi.org/10.1007/978-3-642-00487-2_43},
note = {10.1007/978-3-642-00487-2_43},
year = {2009}
}
```

Carles Martínez García

Bellaterra, July 2011