Semi-automatic Generation of OrBAC Security Rules for Cooperative Organizations using Model-Driven Engineering

Irvin Dongo and Vanea Chiprianov
LIUPPA, University of Pau, Anglet, France

Keywords: Interoperability, Access Control, OrBAC, MDE, Ontology Matching.

Abstract: In an environment of increasing cooperation and interoperability, organizations share resources and services between them to increase their return on investment. But to control the use of shared resources, it is necessary to apply access control policies which are related to how organizations control and secure their scenarios of cooperation. In this paper, we perform a Systematic Literature Review on the current solutions to define access control policies for cooperative organizations. As a result, we identify limitations such as manual negotiation for establishing policies. To address these limitations, we introduce the Semi-Automatic Generation of Access Rules Based on OrBAC (SAGARBO) component which allows semi-automatic generation of security rules based on Model-driven engineering. This reduces negotiation time and the work of the security administrator.

1 INTRODUCTION

Organizations exchange services to obtain benefits such as increased profit or quality of the final product or service. These services involve users, different kind of resources. But for cooperation to be successful it is necessary to control the use of services and other resources. For this, one of the most common mechanisms used is access control. An access control policy allows authorization or denial of the use of resources by a consumer organization. Describing access control policies for cooperative organizations consists in establishing several security rules that have to be accepted and verified by each cooperative organization. Conflicts can arise between these security rules. There can also exist redundant rules. Verifying such rules when the number of cooperative organizations is big, results in a lot of work for the security administrators of each organization.

For organizations to cooperate, they need to interoperate. To have secure cooperation, we need to address interoperability between organizations' access control policies. Consequently, our research question is *how to define security rules for access control that ensure interoperability between organizations*?

An important mechanism in access control is Role Bases Access Control (RBAC), where the security policy defines authorizations to roles and users acquire permissions that are assigned to their roles. However, in the context of interoperability, the main entity is organization. In the work of (Kalam et al., 2003), the concept of Organization is added to RBAC, resulting in OrBAC. This introduces the main features for a secure communication between organizations. It is possible to manage multiple security policies associated with different organizations.

In (Muante-Arzapalo, 2014), the author compares different access control models and concludes that the OrBAC model is the only one that has the concepts of all the other models and additionally new concepts such as Organization, Prohibition, Delegation and Rule prioritization. That is why OrBAC is semantically, the richest model. Another advantage is the fact that there are tools for managing security rules based on OrBAC, for example, MotOrBAC[1].

However, most recent works that use OrBAC security rules for organization interoperability, have limitations related especially to the *manual establishment of the policies*, which makes the work of the security administrator longer. To address this, we propose a component which, using Model Driven Engineering and ontology matching techniques, semi-automatically generates such security rules.

In section 2 we present a literature review about interoperability of OrBAC access control policies. In section 3, we introduce our proposal, its requirements, architecture and implementation. To showcase it, we present a medical case study in section 4.

[1] http://orbac.org/?page_id=12

Dongo, I. and Chiprianov, V.
Semi-automatic Generation of OrBAC Security Rules for Cooperative Organizations using Model-Driven Engineering.
In *Proceedings of the 11th International Conference on Evaluation of Novel Software Approaches to Software Engineering (ENASE 2016)*, pages 43-50
ISBN: 978-989-758-189-2

2 STATE OF THE ART

To have a complete view of the works developed on the issue of cooperation and interoperability between organizations and OrBAC access control policies, we performed a literature review in the repositories: Scopus, ACM Digital Library, IEEEXplore, SpringerLink, ScienceDirect. This allows finding related works to our research question - how to define security rules for the OrBAC access control model that insure interoperability between organizations.

We use the keywords "OrBAC interoperability" because the "OrBAC" model contains the entity Organization which is essential for our research question; and "interoperability" because it is related to cooperation between organizations.

After searching the databases using the chosen keywords, we obtained 95 papers. Among the search results, after reading the title, keywords, and abstracts, and applying the following exclusion criteria:

1. Related to OrBAC as a extesion or based on this
2. Context of System to System
3. Access control for organizations

we selected 17 papers. By analyzing their references, we found one additional paper.

Figure 1 shows the sequence of work carried out from 2005 until 2015 (October), organized into 3 groups. OrBAC was introduced in a paper in 2003 (Kalam et al., 2003) and the first work on OrBAC interoperability appears in 2005. The works inside each group of Virtual Organizations and respectively Web Services share the same architecture. Other works in the Mixed Works group, all have different architectures. A branch in each group presents the works that are based on previous works in the same branch.

2.1 Virtual Organizations

Several works use Virtual Organizations (VO) as a starting point to establish access control. A VO allows interaction between cooperative organizations to share resources in order to accomplish common goals.

Using VOs, (Nasser et al., 2005a) emphasizes the need to establish boundaries between users and resources introduced by various partners in an entrusted environment. The author proposes a new method to automate the creation of VOs based on OrBAC. However, the negotiation between organizations is manual and the time to establish common security rules for this collaboration is long. In (Nasser et al., 2005b) a new method, based on (Nasser et al., 2005a), is introduced to dynamically build VOs based on OrBAC. The proposal mentions the negotiation process but does not specify how it is done.

(Cuppens et al., 2006) propose an OrBAC extension adding new predicates - Organization to Organization (O2O). The main advantage is that each organization can maintain the same roles without needing to add new or existing roles. But to find such compatibility it is required to perform a manual process in the same way as the negotiation process.

The work of (Coma et al., 2008) is based on (O2O) (Cuppens et al., 2006). Additionally, the authors propose different types of compatibility relations between entities. To discover them, "ontology mapping" is used. The main advantages are a detailed access control management and maintaining the computational time of the derivation process polynomial.

(Coma-Brebel et al., 2008) provides a context ontology to be combined with an ontological representation of the OrBAC model. It can handle different types of context such as time, space, but also increases the work of security administrators to establish security policies. In (Coma et al., 2010), there is a detailed explanation of the work of (Cuppens et al., 2006), (Coma et al., 2008) and (Coma-Brebel et al., 2008). It proposes other steps such as license, management policy, privacy, type of communication between organizations P2P (Peer to Peer).

(El Maarabani et al., 2011) propose to verify security requirements by transforming security rules (O2O) to "Linear Temporal Logic" (LTL), thus detecting real-time conflicts and violations of rules.

In this group of VOs, we can mention as main drawback of all approaches, the need to create a new VO for each cooperation. Also establishing the security rules is the responsibility of the administrator.

2.2 Web Services

From the analysis of the state of the art, we identified another group of works, based on Web Services. Web Services offer more flexibility and quality at runtime for choosing or changing services that cooperate.

(El Kalam et al., 2007) proposes an open, distributed and collaborative web services environment for interoperability between organizations, which contains a new model and mechanism called "Poly-OrBAC". Its main advantage is allowing each system to manage their own resources, services, security policies, etc. However, establishing a security policy needs a manual negotiation process.

In (Baina et al., 2008) the authors use the work of (El Kalam et al., 2007) to handle security in critical systems. However, each organization is responsible for the authentication of users when they access the services of other organizations. (Kalam et al., 2009), applies the concepts from (El Kalam et al., 2007)

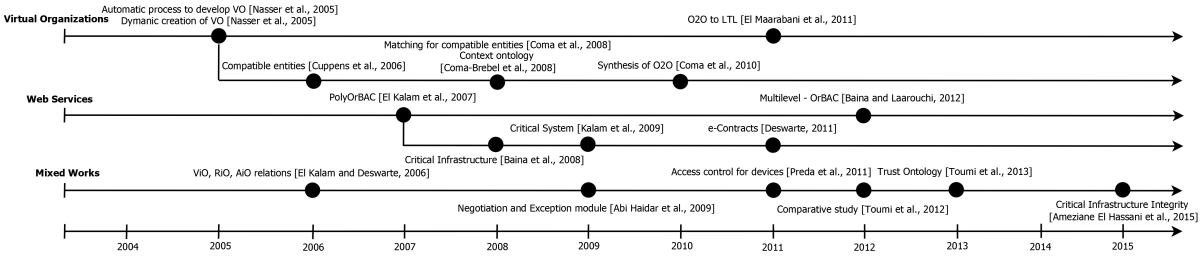

Figure 1: State of the Art.

to critical systems. For interoperability it is necessary to create new security rules. However, this process is performed manually and it is often difficult for the security administrator. (Deswarte, 2011) continues in the environment of critical infrastructures and addresses similar problems as those in (Baina et al., 2008). The authors propose to add "e-Contracts" to PolyOrBAC to express and check the interaction of web services. In the work of (Baina and Laarouchi, 2012) an extension of OrBAC, joined with the Totel integrity model, is presented. The authors address the OrBAC limitation about it not guaranteeing the integrity against corruption of the entity Object.

As a general limitation of works using web services, we found that the way to establish security rules remains manual. For this reason the security administrator needs to invest a lot of effort and time for establishing or defining them.

2.3 Mixed Works

In this group we find other related OrBAC proposals that extend the model or apply its concepts to related issues such as communication between devices, etc.

(El Kalam and Deswarte, 2006), continue working in the context of access control policies for collaborative, heterogeneous and distributed systems. They extend OrBAC adding concepts "View in Organization" (ViO), "Role in Orgazanition" (RiO) and "Activity in Organization"(AiO), which are new relationships respectively between the entities View, Role and Activity and the entity Organization. It allows to manage security policy in detail but increases the complexity.

On the other hand (Abi Haidar et al., 2009) focuses on the negotiation process. They propose an architecture with negotiation and exception treatment modules. However, to get a positive result a long time is required in many cases.

In the work of (Preda et al., 2011) the authors address the control of security of devices between organizations. It improves the OrBAC model by integrating concepts of action specification languages, so as to enable reasoning about the evolution of the policy status as soon as actions are detected. One of the main disadvantages is that there can be lag time between devices, in addition to being able to introduce "DoS" attacks on the PDP (Policy Decision Point).

(Toumi et al., 2012) performed a comparative study between different proposals based on existing models such as RBAC and OrBAC. They identify 3 groups with similar characteristics based on dynamism, abstraction, management complexity and expressibility. In the first group, called Super Organization, they analyze Multi-OrBAc, TeaM based Access Control (TMAC). In the second group, they analyze the proposal O2O which is also analyzed by us. Another group is based on different technologies such as Poly-OrBAC and OrBAC in VOs.

In the context of trust related to distributed systems, (Toumi et al., 2013) proposes a trust ontology based on OrBAC. A trust framework allows us to have more dynamic and interactive policies.

When addressing secure interoperability between organizations, their credibility, critically, integrity are highly important. An extension of OrBAC that takes into consideration these integrity issues is advanced in (Ameziane El Hassani et al., 2015).

2.4 Discussion

As observed in the analysis of the state of the art, there are two main types of realizing secure environments: virtual private organizations and Web services. Both have advantages and disadvantages, but the choice between them often depends on what organizations want to share. For example, if we need a closed secure environment, we should use a virtual private organization, but lack of flexibility is a disadvantage in this kind of cooperation. However, Web services can have a flexible and dynamic cooperation.

An important point is the process of negotiation between the different organizations, which tends to be manual (Nasser et al., 2005a), (Nasser et al., 2005b), (Cuppens et al., 2006) and in many cases, only provide the high level description of the negotiation process without detailing how this can be done (Nasser et al., 2005a), (Nasser et al., 2005b), (Coma et al., 2008) and (Coma et al., 2010). This is a limitation

of the proposed works, because in an environment of cooperation, the negotiation process is complicated.

It is important to emphasize the role of the security administrator in interoperability - to grant access to resources of the organization. This is discussed in works such as (Coma-Brebel et al., 2008), (Kalam et al., 2009), which propose giving the security administrator more responsibilities to define fine-grained security rules. This will further complicate their tasks. Whereas, our contribution will reduce their work.

In this section, we presented our literature review. A related work of survey was performed by (Toumi et al., 2012), presented in *Mixed Works*. They identify 3 groups, like us, but different from ours. The authors conclude that each solution may improve its performances by adapting some other approaches; on the other hand, the administration of security policies would become more difficult, just as we identified.

After analyzing the state of the art, we identified 2 main limitations about the manual negotiation process and the work of the administrator. We focus on increasing the automatization degree of the negotiation process between cooperative organizations in order to facilitate the work of the security administrator.

Furthermore, ontologies are also presented in security policies (Coma et al., 2008), (Coma-Brebel et al., 2008), (Coma et al., 2010) to model organization knowledge and information. Due to the fact that ontologies can be used to describe and analyze knowledge, we use them to discover the similarities of certain types of entities in organizations.

3 PROPOSAL: GENERATING SECURITY RULES

As a solution to the problems identified in the state of the art, we generate semi automatically access control rules to resources from existing rules within the organization that provides these resources. For this, we focus on similar roles in different organizations. We describe roles, actions and resources of each organization using ontologies and discover similarity between roles using ontology matching algorithms.

To develop our proposal, we use a software engineering approach, starting from requirements, through architecture and implementation.

3.1 Requirements

We identified the following requirements from our analysis of the state of the art:

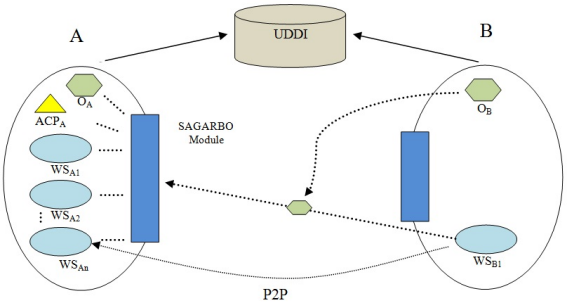

Figure 2: Interoperability Architecture for access control rules generation.

- Interoperability architecture, a requirement coming from our research questions.
- Access control policies based on OrBAC, to preserve the security of resources within organizations, security policies that restrict access and use of the resources are necessary.
- Describing organization entities, we consider that similar roles in two organizations will have similar security rules.

3.2 Architecture

In order to fulfill the identified requirements, we propose the architecture that follows. To satisfy the interoperability architecture requirement, we decide to base our architecture on the Service Oriented Architecture (SOA) paradigm. This places our proposal in the category of works that we identified in the state of the art, dealing with web services. Our OrBAC requirement means that our architecture needs to generate new OrBAC access control policies. To answer the requirement of describing organization entities, one common way to describe semantics of web services and the context in which these operate inside the organization, is ontology.

3.2.1 Structural Architecture

In figure 2, we present the structure of our architecture. Organization B consumes a web service of A. Organization B discovers the web service which best satisfies its requirements (WS_{A2}). This process uses the UDDI repository. After that, to enable cooperation among them, organization B sends A a request to use its web service. Together with this request, it also sends its ontology describing its resources (O_B). Organization A receives this request and its Semi-Automatic Generation of Access Rules Based on OrBAC (SAGARBO) component analyzes it.

This architecture has the novelty of using a new component that we call SAGARBO. The SAGARBO

component works with the ontology and the access control policy of organization A (ACP_A) and the ontology of organization B to generate security rules for organization A (provider), using Model-driven engineering. We will explain more about it in Section 3.4. Organization B also has a SAGARBO component because it can offer its web services and other resources to other organizations. However, this component is mandatory when organization B is just the provider.

3.2.2 Behavioral Architecture

After presenting the structure of our architecture, we focus on its behavior. For this, we introduce a process based on (El Kalam et al., 2007).

Phase 1:

1. Each organization that wishes to provide services, must publish them in a web service registry, for example UDDI.
2. Other organizations may discover and use the web service.
3. Organizations negotiate among themselves. For this, the consumer organization shares its public information in one ontology, especially the resources it needs and does not have. The provider organization uses matching algorithms to find similarity between entities requested by the consumer and those that belong to the provider.
4. Organizations establish a technical contract (based on the legal one) and jointly define security rules. In the negotiation process, by applying a matching algorithm between entities, SAGARBO generates a list of new security rules for the provider, using its existing rules.
5. From the list of new security rules, the administrator decides which rule can be selected in accordance with the previously established contract.

Phase 2: At runtime, if a user wants to perform an activity and requires any resource of the web service, the provider organization checks the user's identity and makes a decision based on its security policy and the role of the user. It finally authorizes or denies access. This is done through a Peer to Peer protocol (P2P), i.e. using a direct connection after all the steps of the first phase have been performed.

3.3 Ontology and Ontology Matching

An ontology allows to describe knowledge in a particular area using a specific vocabulary. The vocabulary describes the conceptual elements and relationships between them (Chandrasekaran et al., 1999). To find similar entities in ontologies from different organizations, it is necessary to use matching algorithms. For our requirement of similarity between entities, we analyzed ontology matching approaches based on systematic literature reviews, such as (Choi et al., 2006) and (Pavel and Euzenat, 2013). In the work (Pavel and Euzenat, 2013), there is an analysis of the most recent matching tools (SAMBO, Falcon, DSSim, RiMOM, AsMOV, Anchor-Flood and Agreement Maker); this is the reason why we have chosen to analyze the tools reviewed in this work. To choose a particular tool for our proposal, we have established the following selection criteria:

- The ability to read an OWL format because ontologies are commonly described in this format.
- A terminological analysis because it is a fundamental technique to find similar terms.
- Structural analysis - recognizing similar substructure between properties.
- Semantic analysis increases the success percentage but also increases the complexity of the tool.
- Free access, but not necessarily open source - because we are not interested in developing or extending an ontology matching tool.
- A graphical interface would facilitate tool use.

The ones that meet our minimum selection criteria of lexical and structural analysis are: Sambo, Falcon, DSsim, AsMOV and Agreement Maker. Regarding the free access criterion, only Falcon meets it. Therefore, if we want to take in account the semantic criterion as well, there are still no tools that satisfy it. In conclusion, we retain Falcon.

Falcon allows us to see the similarity between the entities of 2 ontologies. The minimum similarity value is 0 and the maximum 1. As the two ontologies are different, it is improbable to find two entities with similarity 1. That is why we have to define a threshold above which we consider the entities to be similar. This threshold generates more or less rules depending if it is closer to 0 or to 1, respectively.

3.4 Model Transformation

In Model-driven engineering (MDE), models conform to Meta-Models (MM), like a program conforms to the grammar of the programming language. A Model Transformation (MT) is the automatic generation of target model(s) from source model(s), according to a set of transformation rules.

We are defining an MT to generate the access control policies for the provider organization. It takes as inputs the access control policies of the provider and

the list of matching roles from the consumer with similar roles from the provider and generates the new access control policies for the provider. The access control policies, for both consumer and provider organizations, conform to the OrBAC MM, and the matching list conforms to the MM used by Falcon.

The generated access control policies are presented to the security administrator, who decides which to keep. Through repeated trial and error, the administrator determines which threshold to use.

4 CASE STUDY

In the health domain, there are several actors, some of them in different organizations. Each of them may need permissions and/or restrictions to access resources such as medical records, prescriptions.

Our case study is based on the SELKIS[2] project. From this, we focus on two medical organizations: Radio3D and HealthCare and a web service called HealthCareWebService (HCWS) provided by HealthCare. Radio3D is an enterprise that provides services of radiology and technology for making diagnoses. HealthCare is a government hospital that has patient records and shares them with other institutions in the same field. HCWS allows us reading and modifying information and medical records of patients.

The establishment of the secure cooperation between these two organizations follows our proposal and is described in the following subsection.

4.1 Cooperation Scenario

A patient goes to HealthCare for a routine control. The doctor asks for an exam consisting of X-Rays.

The patient chooses Radio3D. (S)he goes to the medical secretary, who opens a session in the Radio3D software and searches the patient's ID in the system. (S)he cannot find the patient so (s)he opens the registration form to create a new record. *The registration form uses the HCWS to automatically read the patient's public information from HealthCare and write it in the Radio3D software*.

Later, the Radio3D radiologist performs a diagnostic based on the X-Rays images. This diagnostic also *takes into account the medical record of the patient in the HCWS in order to have greater support in the diagnostic*. When the diagnostic is complete, *the radiologist stores it as a result in the Radio3D software and sends this information to the HCWS, to store it*. When the patient goes back to HealthCare,

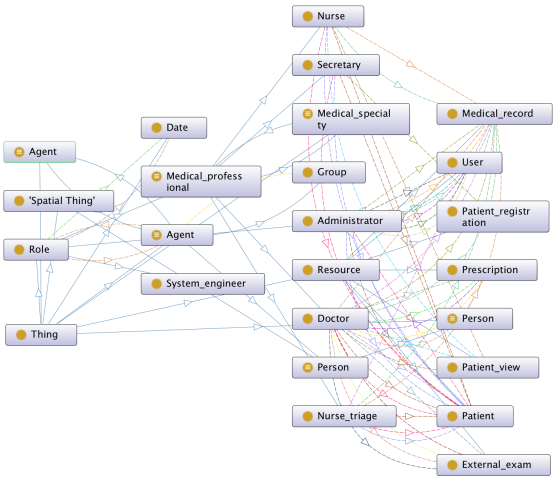

Figure 3: HealthCare Ontology.

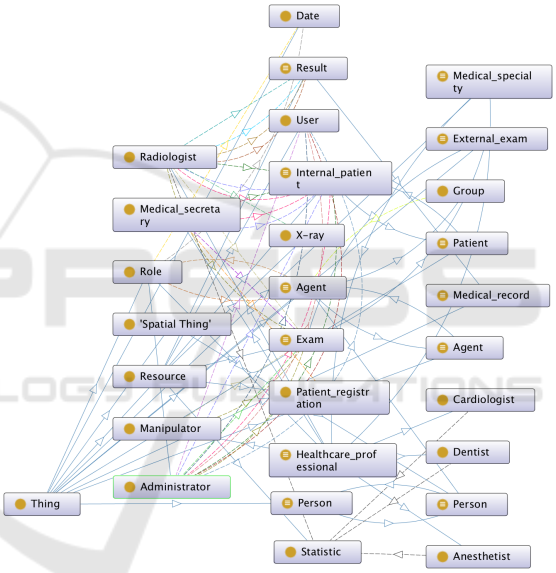

Figure 4: Radio3D Ontology.

the doctor will have the diagnostic of the X-Rays and (s)he can take the best action for the illness.

In HealthCare, there are 24 security rules, inspired from the SELKIS project. For our scenario, the Radio3D secretary needs the authorization to read the public information of the patient. Also, the Radiologist in Radio3D needs the access right to read a Medical Record and to add the results of the analysis. In total, it is necessary to add three new security rules in order to satisfy the cooperation requirements.

4.2 Ontologies

For developing the ontologies, we used Protégé[3] a

[2] lacl.univ-paris12.fr/selkis

[3] http://protege.stanford.edu/

free, open-source ontology editor. They contain and describe entities like Role, Resource, actions, used in defining and generating access control policies. The ontologies are based on Participation Schema[4] and some properties of the FOAF vocabulary[5].

In figure 3, the ontology of the HealthCare organization is presented. There are two main entities: Resource and Role. The relations between resources and roles represent the actions the roles can execute on the resources. These may be of type: "read", "add", "modify", "delete", "search". Figure 4 describes the same for the Radio3D ontology. In the same way for the Radio3D ontology, figure 4, we can see resources, roles and relations as actions.

4.3 Experiments and Generated Access Control Rules

We tested our solution in two different cases. In the first one we generated security rules which have a high probability to be accepted by the security administrator because in the ontology matching step, the roles have a high similarity, and they can even be equivalent or equal. Therefore in this case we fix the similarity threshold to 0.75. Security rules generated by this matching threshold are most often retained by the administrator, but it is possible that other security rules are required. So this high threshold may generate a pertinent but most likely incomplete set of security rules. Thus the administrator may need to write additional security rules, which demands a relatively high cognitive effort.

In the second case, we produce a greater amount of security rules. The administrator will have more choices. This increases the time they spend on selecting the security rules, but decreases the time and effort spent on writing additional rules. Therefore, this case may further facilitate the work of the security administrator. In this case, we fix the threshold to 0.35.

4.3.1 Generated Access Control Rules for Threshold 0.75

For the threshold 0.75, our approach generates 8 new security rules because of the similarity between the roles Administrator (HealthCare)- Administrator (Radio3D) and Secretary (HealthCare) - Medical Secretary (Radio3D). We obtain the new generated rules: Radio3D_ Medical_secretary_ 1, Radio3D_ Medical_secretary_ 2, Radio3D_ Administrator_ 1, Radio3D_ Administrator_ 2, Radio3D_ Administrator_ 3, Radio3D_ Administrator_ 4, Radio3D_ Administrator_ 5, Radio3D_ Administrator_ 6. The security administrator chooses the security rules that satisfy the cooperation. However, only one such rule is generated - the authorization for the Medical Secretary to read public information of the patient in HeathCare organization. The security administrator has to create two other security rules.

[4]http://vocab.org/participation/schema-20080925

[5]http://xmlns.com/foaf/spec/

4.3.2 Generated Access Control Rules for Threshold 0.35

For the threshold 0.35, we obtained 16 new security rules for the similarity between roles Administrator(HealthCare) - Administrator (Radio3D), Secretary (HealthCare) - Medical Secretary(Radio3D) and Doctor(HealthCare) - Radiologist (Radio3D). In this case, the security administrator chooses the new rules for the cooperative scenario and (s)he finds all the 3 required security rules.

5 CONCLUSION

In this paper we investigated the issue of defining security rules for access control to ensure interoperability between organizations. We performed a literature review on OrBAC-based cooperation.

This allowed us to refine the research question and focus on the issues of the manual negotiation process and reducing the work of the security administrator.

To solve these problems, we proposed an architecture based on the work of (El Kalam et al., 2007). It introduces the Semi-Automatic Generation of Access Rules Based on OrBAC (SAGARBO) component that allows the provider organization to semi-automatically generate security rules. For this, we use model driven engineering and ontology matching. We developed a case study based on the Selkis project. We describe the needs of the organizations, as well the roles, actions and resources using ontologies and security rules. Using the ontology matching tool Falcon, which we selected, we detect the entities which have a similarity greater than a certain threshold.

Our proposal can be classified as part of the Web Services group of works which we identified in the state of the art. The works in this group are mainly based on PolyOrBAC. Like PolyOrBAC, our approach uses an open, distributed and collaborative web service environment. However, where PolyOrBAC employs a manual negotiation process, we use a semi-automatic generation approach in order to facilitate the work of the security administrator.

Our proposal uses a similarity threshold less than 100%. That is why it is not completely certain that a

totally automatic generation process of security rules could ensure the security of all resources. Therefore the ultimate validation of the security rules is the decision of the administrator. However, even if the security administrator has to define some of the security rules, their effort of creating them is still reduced.

A limitation of our approach is the sharing of information in the ontology of the consumer organization. This ontology may include essential and sensitive information of the organization. Regarding the ontology matching, it is possible to apply other methods and tools, which may increase the accuracy of the results. For the moment we only use roles for the matching analysis, but other entities like resources and actions could be used to improve the similarity.

REFERENCES

Abi Haidar, D., Cuppens-Boulahia, N., Cuppens, F., and Debar, H. (2009). Xena: an access negotiation framework using xacml. *Annales des télécommunications-Annals of telecommunications*, 64(1-2):155 – 169.

Ameziane El Hassani, A., Abou El Kalam, A., Bouhoula, A., Abassi, R., and Ait Ouahman, A. (2015). Integrity-orbac: A new model to preserve critical infrastructures integrity. *Int. J. Inf. Secur.*, 14(4):367–385.

Baina, A., Kalam, A., Deswarte, Y., and Kaaniche, M. (2008). Collaborative access control for critical infrastructures. In Papa, M. and Shenoi, S., editors, *Critical Infrastructure Protection II*, volume 290 of *The International Federation for Information Processing*, pages 189–201. Springer US.

Baina, A. and Laarouchi, Y. (2012). Multilevel-orbac: Multi-level integrity management in organization based access control framework. In *Multimedia Computing and Systems (ICMCS), 2012 International Conference on*, pages 933–938.

Chandrasekaran, B., Josephson, J. R., and Benjamins, V. R. (1999). What are ontologies, and why do we need them? *IEEE Intelligent Systems*, 14(1):20–26.

Choi, N., Song, I.-Y., and Han, H. (2006). A survey on ontology mapping.

Coma, C., Cuppens-Boulahia, N., and Cuppens, F. (2010). Secure interoperability with o2o contracts. In *Web-Based Information Technologies and Distributed Systems*, volume 2 of *Atlantis Ambient and Pervasive Intelligence*, pages 257–292.

Coma, C., Cuppens-Boulahia, N., Cuppens, F., and Cavalli, A. R. (2008). Interoperability of context based system policies using o2o contract. In Chbeir, R., Dipanda, A., and Yétongnon, K., editors, *SITIS*, pages 137–144. IEEE Computer Society.

Coma-Brebel, C., Cuppens-Boulahia, N., Cuppens, F., and Cavalli, A. R. (2008). Context ontology for secure interoperability. In *ARES 2008 : Third international conference on availability, reliability and security*.

Cuppens, F., Cuppens-Boulahia, N., and Coma, C. (2006). O2o: Virtual private organizations to manage security policy interoperability. In Bagchi, A. and Atluri, V., editors, *Information Systems Security*, volume 4332 of *LNCS*, pages 101–115.

Deswarte, Y. (2011). Protecting critical infrastructures while preserving each organization's autonomy. In Natarajan, R. and Ojo, A., editors, *Distributed Computing and Internet Technology*, volume 6536 of *LNCS*, pages 15–34.

El Kalam, A., Deswarte, Y., Baina, A., and Kaaniche, M. (2007). Access control for collaborative systems: A web services based approach. In *Web Services, 2007. ICWS 2007. IEEE International Conference on*, pages 1064–1071.

El Kalam, A. A. and Deswarte, Y. (2006). Multi-orbac: A new access control model for distributed, heterogeneous and collaborative systems. In *8th IEEE International Symposium on Systems and Information Security*.

El Maarabani, M., Cavalli, A., Hwang, I., and Zaidi, F. (2011). Verification of interoperability security policies by model checking. In *High-Assurance Systems Engineering (HASE), 2011 IEEE 13th International Symposium on*, pages 376–381.

Kalam, A., Baida, R., Balbiani, P., Benferhat, S., Cuppens, F., Deswarte, Y., Miege, A., Saurel, C., and Trouessin, G. (2003). Organization based access control. In *Policies for Distributed Systems and Networks, IEEE 4th Intl Wksh on*, pages 120–131.

Kalam, A. A. E., Deswarte, Y., Baina, A., and Kaâniche, M. (2009). Polyorbac: A security framework for critical infrastructures. *International Journal of Critical Infrastructure Protection*, 2(4):154 – 169.

Muante-Arzapalo, D. Y. (2014). *Une approche base sur l'Ingénierie Dirigée par les modèles pour identifier, concevoir et évaluer des aspects sécurité*. PhD thesis, Université de Pau et des Pays de L'Adour.

Nasser, B., Laborde, R., Benzekri, A., Barrère, F., and Kamel, M. (2005a). Access control model for inter-organizational grid virtual organizations. In Meersman, R., Tari, Z., and Herrero, P., editors, *On the Move to Meaningful Internet Systems 2005: OTM 2005 Workshops*, volume 3762 of *LNCS*, pages 537–551.

Nasser, B., Laborde, R., Benzekri, A., Barrere, F., and Kamel, M. (2005b). Dynamic creation of inter-organizational grid virtual organizations. In *e-Science and Grid Computing, 2005. First International Conference on*, pages 8 pp.–412.

Pavel, S. and Euzenat, J. (2013). Ontology matching: State of the art and future challenges. *IEEE Trans. on Knowl. and Data Eng.*, 25(1):158–176.

Preda, S., Cuppens, F., Cuppens-Boulahia, N., Garcia-Alfaro, J., and Toutain, L. (2011). Dynamic deployment of context-aware access control policies for constrained security devices. *Journal of Systems and Software*, 84(7):1144 – 1159.

Toumi, K., Andrés, C., and Cavalli, A. R. (2013). Trust ontology based on access control parameters in multi-organization environments. In *SITIS*, pages 285–292.

Toumi, K., Cavalli, A., and El Maarabani, M. (2012). Role based interoperability security policies in collaborative systems. In *Collaboration Technologies and Systems (CTS), 2012 International Conference on*, pages 471–477.