Representing User Privileges in Object-Oriented Virtual Reality Systems

Adam Wójtowicz and Wojciech Cellary

Department of Information Technology, Poznań University of Economics
{awojtow,cellary}@kti.ue.poznan.pl

Abstract. In virtual reality systems which are collaborative and dynamic, i.e. where at run-time mutually interactive objects can be added or removed in different contexts and where their behavior can be modified, the problem of data security and privacy protection is renewed. In such virtual worlds operations on objects should or should not be allowed to users playing particular roles with respect to inter-object interactions. In this paper a method called VR-PR is presented, where privileges are represented by pairs: object – semantic operations induced from object interactions. Semantic operations are generated using automatic analysis of the object method call graphs. Then they are used in the privilege creation and modification process. Privileges based on semantic operations are expressive, flexible and consistent with permanently evolving set of objects composing the virtual world, interactions between the objects, and a set of users.

Keywords: User privileges, virtual reality, data security, data privacy, semantic operations.

1 Introduction

Today virtual worlds are dynamic environments where multiple objects interact with each other by calling methods in reaction to internal and external events. Virtual worlds are also creative environments, where at run-time users create new objects, modify them, assemble them into more complex objects, extend their functionality etc. In such dynamic and creative environments the problem of data privacy protection is renewed. From the business perspective, intellectual property rights of creators and publishers of objects in virtual worlds must be protected, as they are source of revenues. Thus, flexible access control using privileges based on interactions existing in a persistently running virtual world should be installed. Privileges granted to a user for a given object should be represented in a way that is compatible with the representation and semantics of intellectual property rights issued for this object. Also, the semantics of interactions between objects owned by different users should be taken into account by the privilege system. Moreover, the privilege system should automatically encompass newly created objects. In virtual worlds objects may be created from scratch by a user who becomes their sole owner, but also as compositions of preexisting objects coming from different sources. The privilege system should be expressive

L.M. Camarinha-Matos, P. Pereira, and L. Ribeiro (Eds.): DoCEIS 2010, IFIP AICT 314, pp. 52–61, 2010.

enough to handle such dependencies. Methods of privilege modeling developed so far, which are presented in Section 3, are either geometry-centric with no advanced interaction support or coarse-grained with no privilege semantics modeling capabilities. Those methods however are not sufficient for highly dynamic creative virtual worlds.

In this paper, a method called VR-PR is proposed of flexible user privilege representation for virtual world objects, maintaining compatibility with access control standards and the data model. The concept of this method is presented in Section 2. In Section 3 the state of the art in the field of access control models which can be applied to multi-user virtual worlds is presented, followed by critical remarks. In Section 4 VR-PR approach is presented to privilege representation and generation of semantic operations used to express privileges. In Section 5 the main issues concerned in this paper are discussed. Section 6 concludes the paper.

2 Contribution of the VR-PR Method to Technological Innovation

The VR-PR method concerns flexible user privilege representation for virtual world objects. The VR-PR method consists of automatic analyses of relationships and interactions between objects of a dynamic virtual world constructed according to the object-oriented data model, such as the one presented in [7]. To this end, a semantic layer is inserted between the access control mechanism and the object-oriented data model. The semantic layer reflects real interactions between objects, represented by a set of abstract semantic operations. The set of semantic operations may slowly evolve over time. Its evolution is, however, much more stable than transformations of the virtual world objects, interactions and structure. In the VR-PR method two phases are alternately performed during virtual world run-time: the phase of automatic generation of semantic operations and the phase of privilege creation and modification. To guarantee consistency of semantic operations used during the second phase in the first phase semantic operations are created basing on automatic analysis of object method call graphs.

The following is an innovative contribution of this paper to the area of virtual world security. First, an access control model is proposed appropriate to a virtual world containing very large number of VR classes, objects and methods that is understandable and manageable for non-IT professional users who may express their will in terms of intuitively understandable semantic operations instead of object methods.

Second, a privilege system is proposed that strictly controls the allowed range of virtual world penetration by behavioral method calls. Third, an algorithm for automatic regeneration of semantic operations used in privileges is proposed, which assures privileges consistency with the data model and its integrity. It increases the security level of the security policies defined using privileges containing semantic operations.

Fourth, a two-phase induce-and-use approach is proposed, which makes the process of privilege management stable: operation set is updated on-demand, but the updates do not change as fast as the data model evolves. Semantic operations can be regenerated without modifying the existing privileges, as well as without role-privilege and user-role assignment modifications.

3 State of the Art

When designing virtual worlds, to control access to objects Role-Based Access Control (RBAC) model [16], Attribute-Based Access Control (ABAC) [17], extensions of these models or their combinations may be applied. Although they are useful in the virtual worlds domain as far as roles, users and their credentials are concerned, they do not solve the problem of privilege granting in highly dynamic virtual worlds.

Research on data privacy protection in virtual environments is derived from the output of either CAD or VR communities. The majority of research effort on advanced privileges modeling in virtual environments is based on the CAD achievements as there is a need in the industry for CAD systems providing data privacy protection while enabling safe collaboration. In [1] a role-depended access model to 3D environments is proposed. In this approach each design feature of an object is assigned to one of predefined access levels representing modes of detail reduction. The role is defined by selecting access level for each object. It protects object geometry only – protection does not concern interactions and behaviors. Users update objects independently, then objects are synchronized by the central system. Such asynchronous approach is justified in some CAD collaborative applications, but it does not meet virtual worlds practice. In [2] an access control model for distributed 3D collaborative engineering systems is proposed. In this model RBAC extension is used which consists of a partial data sharing mechanism and fine grained access control. Access granularity is supported on different levels: assembly, component, feature and surface, which form a hierarchy. Dynamic geometric and non-geometric constraints can be modeled, but inter-object interactions and their different semantics are not supported as an element of the privilege system. Only basic operations such as read, write and modify are used to form privileges. In [3] FACADE system is proposed, which is synchronous collaborative 3D virtual environment enabling selective sharing of 3D objects. FACADE authors classify their work as both data- and interaction-centric, however, interaction is regarded here only as inter-user design-time interaction and not inter-object dynamic behavior. There are cross-hierarchy relations between objects called "need-to-know requirements" but their nature is static and they are explicitly defined by designers. This concept provides role-based views on modeled data with read/write privileges granularity. Read privilege is extended to a continuous scale of mesh resolutions, but since only geometry is considered, there is no support for a whole spectrum of semantic operations that could form privileges.

From among non-CAD-based approaches, the most distinguished are rule-based access control models developed for the multimedia domain as a whole. Such models have even been a subject of standardization as a part of MPEG-21 – Right Expression Language (REL) [18]. Unfortunately, Digital Item (DI) representation which lies under it is not expressive enough to support complex behavior-rich 3D objects. Other access control standards, such as Extensible Access Control Modeling Language (XACML) [19], are even more general in the multimedia context.

An interesting rule-based access control model has been developed for and implemented in the DEVA system [5]. In the DEVA approach, execution of a given operation is controlled by access rules expressed by a source code defined in so-called *keys*. However, both operations and keys have to be explicitly defined by users. There is no automatic induction of operation dependencies, so users are responsible for maintaining

access rules consistency. In [5] there is no explanation of how the DEVA approach is integrated with standard access control or how privileges are represented.

A number of papers are devoted to methods of modeling virtual worlds not only as a set of geometrical objects, but also semantically [8,9,10,11]. Such approaches enable application of algorithms automatically exploring the content of the virtual world, reusing objects in different contexts and taking advantage of domain knowledge stored in external ontologies. However, there has been no effort to integrate semantic virtual world models with user privileges control to protect data privacy. The next research field related with this paper is structured design of virtual worlds [7]. It focuses on methods of building VR applications in which content is dynamically configured from high-level elements, thus it can be relatively easily created and modified by domain experts and common users. Nevertheless, those reusable elements lack integrated user privilege support as well.

4 VR-PR Approach

4.1 Concept of the VR-PR Approach

Interactive virtual worlds admit content dynamically generated by users. In such virtual worlds the structure of the data model evolves which entails specific requirements for the access control model. In standard access control models such as RBAC and its extensions, *privileges* are formed as a pair *operation – resource*. However, in dynamic virtual worlds based on object oriented paradigm a question arises: how to build an access control model appropriate to a very large number of dynamic classes, objects and methods that is understandable and manageable for users? In such virtual worlds resources have to be objects, however, operations may be defined differently. If an operation is an object method, privileges are too dependent on the data model. When a method changes, or a new class is added, the operation set used to define privileges has to be changed accordingly. If an operation represents all the object's methods, i.e. privileges are defined with the object granularity, another problem arises: different methods of an object usually have diametrically different semantics and they call different methods (i.e. have different call graphs), so their range of penetration of the virtual world is different, which is not reflected by such privilege system. Moreover, it is also very dependent on data model changes. If an operation is a primitive, such as "read" or "write", privilege system is independent of data model changes, but it does not follow the evolution of the virtual world, so it is useless in case of dynamic virtual worlds that constantly evolve. If the set of operations is not fixed but is updated by human operators according to data model changes, the risk of inconsistencies grows drastically.

In the VR-PR approach, *semantic operations* are used. A semantic operation is a conceptual extension of the operation from the standard access control models. Similarly to a regular operation, it is used to define privileges in conjunction with objects. But the main innovation is its semantics that is automatically induced from the object-oriented data model, instead of being defined arbitrarily. In other words a semantic operation is a set of bindings to semantically similar object methods induced from method call graphs. Each semantic operation is assigned to a given type and it has its

place in the semantic operations hierarchy. Semantic operations reflect all the method calls, i.e. all in-world interactions of the objects, which may be complex, diverse, and dynamic. A semantic operation set is generated in a way assuring that each method call is bound to at least one induced semantic operation. Semantic operations are intuitively understandable by virtual content authors, publishers, administrators or other users authorized to create new privileges or modify existing ones.

In the VR-PR approach the privileges are processed in two phases. The *Semantic Operations Generation Phase* (SOGP) follows the virtual world data model evolution by regenerating a semantic operation set on each change. It is performed by the induction process basing on the analysis of the similarity of virtual object's method call graphs, as well as on the analysis of relationships between elements of the data model (cf. Subsection 4.2). A set of available semantic operations is generated from potential method calls known at design-time (inter-object relationship: uses-a), and from the static class hierarchy and object set structure (relationships: is-a, instance-of, part-of). During the SOGP phase semantic operation type categorization and generalization hierarchies are built.

Semantic operations are induced by *semantic unification* of different methods. This means that methods with similar call graphs are logically bound to a common semantic operation in the privilege system, whereas in the virtual world they are still recognized as separate ones.

From the data security and privacy point of view, measuring the level of similarity of the methods by measuring the level of similarity of their call graphs is justified. A semantic operation which groups methods with similar call graphs describes well the range of the penetration of the virtual world by a set of calls. In the VR-PR approach, the allowed range of virtual world penetration by method calls is controlled by the privilege system. As a result, the privilege function of protecting objects is satisfactory fulfilled – the system is protected against non-authorized deep method calls in a dense net of variable behavioral dependencies.

The second phase of the approach is the *Privilege Creation and Modification Phase* (PCMP), which is described in Subsection 4.3. Semantic operations induced during the first phase are used to form privileges by assigning them to objects. This process is controlled by an access control mechanism which makes the process consistent with the data model.

4.2 The SOGP Phase

In the VR-PR approach semantic operation induction is based on static *call graph* – a graph whose nodes are methods and edges are all possible calls of other methods. A node represents a method in the context of a given object, which means that if a given class has many instances, then for each method of this class there are as many nodes as instances. The call graph is created from the source code of virtual world objects. Global and local call graphs are distinguished. The *global call graph* contains all the methods and all the potential calls of other methods included in the source code of all the objects composing a virtual world at a given moment. It is updated incrementally when the data model changes. A *local call graph* is developed for each method. It is a subgraph of the global call graph built with a given method as the starting point and containing all the methods that are called by these methods, and all their callees.

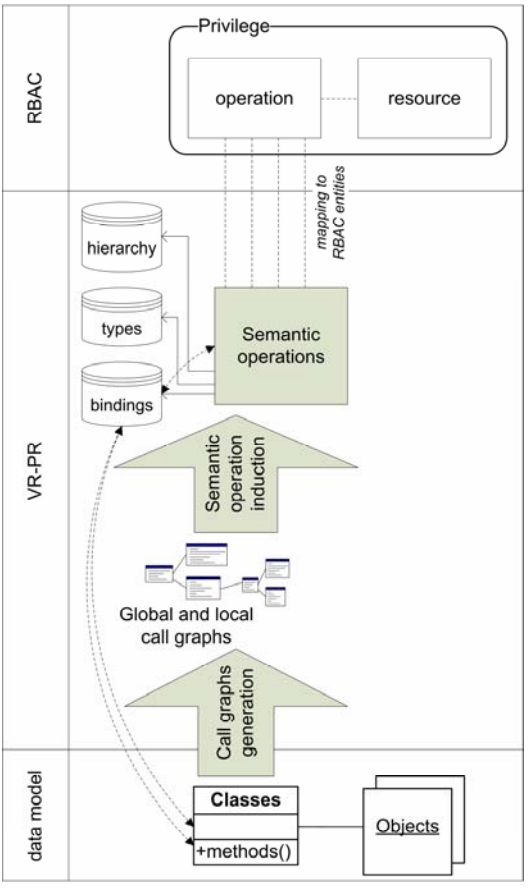

Fig. 1. SOGP: semantic operations generation

Semantic operations have types assigned. The types reflect the way semantic operations have been induced. When a given semantic operation is based on the methods with identical local call graphs, its type is called *fully-matching*. When call graphs of two unified methods cover methods belonging to the same classes (but they are based on different objects sets), the semantic operation is called *class-matching*.

The first phase of the VR-PR approach is composed of the following five steps (Fig. 1):

1. Construct the global call graph. This graph is a basic data structure for the process of automatic generation of semantic operations.
2. Induce semantic operations. The induction of each semantic operation is preceded by local call graph pre-selection. Each semantic operation is generated by semantic unification of different methods, basing on the analysis the similarity of local call graphs of methods and on the analysis of the static class hierarchy and object set structure. Metadata descriptions of the software modules, classes, objects and methods are taken into account during semantic unification if they are available.
3. Assign types to semantic operations.
4. Store bindings between each semantic operation and a set of methods which have been the base of its induction for further use during the PCMP phase.
5. Build semantic operations hierarchy according to composability criterion. It is orthogonal both to the role hierarchy and to the class inheritance hierarchy.

Potentially, semantic unification can be performed on two methods which are: different methods of different classes (but having similar calls); the same method, but in different object context (parameterized or using non-static field values); different methods of the same class. The aforementioned cases are distinguished during the selection of methods to be unified, as well as during call similarity analysis. Metadata descriptions of the software modules, classes, objects and methods taken into account during semantic unifications are useful in excluding semantically incoherent unifications, as well as in providing semantic labeling for the semantic operations.

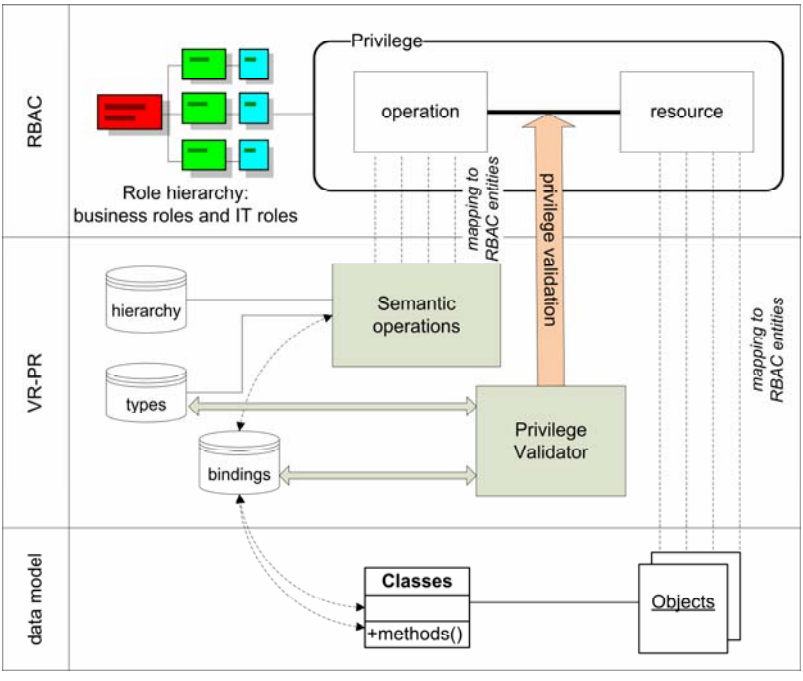

Fig. 2. PCMP: privilege creation/modification

4.3 The PCMP Phase

In the PCMP phase of the VR-PR approach the induced semantic operations are used to create privileges by assigning semantic operations to objects and binding so created privileges to roles (Fig. 2). Whether a given semantic operation may be assigned to a given object or not, depends on the *privilege validation* mechanism. Privilege validation can work in two modes: *strict privileges* and *potential privileges*. In the strict privileges mode a privilege may be created only if a given semantic operation has been induced from the requested object. In the potential privileges mode a given semantic operation can be assigned to an object even if the operation has not been induced from any of the object's methods. Such privileges are used when it can be anticipated that taking into account data model dynamism some objects will gain new competences. However, at the moment of the creation of such privileges they do not make any new method calls allowed, because those methods are as yet inexistent.

Since all the calls which are triggered by a given operation, including all the call dependencies (represented by a call graph), are known before each iteration of the privilege creation phase, during privilege assignment this knowledge can influence final decision whether a given privilege can be assigned or not. Thus, after privilege assignment, during run-time it is guaranteed that no access error will arise related to the lack of privileges to any of dependent methods called. This follows from the fact that each semantic operation stores all the bindings to the methods which were the base of its induction.

5 Discussion

The SOGP and PCMP phases described in Section 4 are following each other at runtime. Creating privileges is not a static task performed only during the virtual world creation, but a dynamic process following virtual world evolution. Users, roles and virtual world data model naturally evolve, while access control model core structures as semantic operations hierarchy remains persistent. In earlier approaches the operation set was static, though operations allowed on resources were defined with different semantics and complexity, i.e. read/ write, or execute/ modify/ insert/ append, or activate/ play/ reorganize. In some cases the operation set could evolve via non-automated changes following data model modifications, which does not assure privileges consistency. In the VR-PR approach, dynamism of the virtual world is inherently taken into account. Defining privileges using automatically regenerated semantic-based operations makes the process of role creation and management consistent, because of semantic operation set internal consistency and consistency with currently used data model. In the VR-PR approach semantic operations layer introduces stability into the process of privilege management. It is updated on-change (i.e. when new objects or new interactions appear), but updates do not change the semantic operations set significantly – especially when semantic operations are induced hierarchically and form a tree structure. Thus, access to semantic operations provides a safe tool to a role manager or any user who is not a 3D modeling expert nor a programmer but who is eligible to create or modify a privilege.

The VR-PR approach makes it possible to avoid unwanted frequent redefining and proliferation of roles. It may happen when privilege changes are not driven by business processes (e.g. a virtual world user gains new duties), but are forced by low level data model activity modification (e.g. when competences of the object to which privileges have been already granted are changed). The advantage of the VR-PR approach is that in this approach semantic operations can be regenerated without modifying the privileges assigned, as well as without role-privilege and user-role assignment modifications.

As an additional benefit, descriptive possibilities of semantic operations can be used in the role-mining process which is performed for security auditing purposes. In the VR-PR approach each semantic operation forming privilege assigned to a role expresses meaningful information about privilege semantics with an explicit representation. Semantic operations used in privileges can be treated as metadata unambiguously describing the role to which those privileges have been assigned. Having such metadata, role-mining process is much more straightforward.

Generally, in object-oriented virtual worlds applications during their lifetime there is a drift towards decreasing the size of the methods and increasing the number of calls. Along with increasing the number of calls, inter-object dependencies become more complex. Thus, a need for automatic analysis for security purposes becomes critical. This is yet another motivation for applying the VR-PR approach to the object-oriented virtual worlds.

6 Conclusions

In the VR-PR approach presented in this paper to provide data security and privacy a security mechanism is proposed based on the concept of semantic operations. They are derived at run-time from the virtual world's current data model and are applicable to access a control model as a part of a privilege. Semantic consistency of the security policies composed of privileges using semantic operations is forced by the two-phase regeneration and validation mechanism. On the other hand, this challenging functionality does not preclude expressing user rights in a precise, accurate, and flexible way.

The VR-PR approach bridges the semantic gap between abstract roles, both business roles and IT roles of virtual world users, and low-level operations executed on virtual world objects. Development of an abstract layer of semantic operations reduces the risk of inconsistent privilege modifications. It does not violate the RBAC access control model nor the object-oriented data model – it constitutes a middle layer placed between these two models developed for different purposes and it is designed with respect to 3D virtual worlds specificity.

References

1. Qiu, Z.M., Kok, K.F., Wong, Y.S., Fuh, J.Y.: Role-based 3D visualisation for asynchronous PLM collaboration. Comput. Ind. 58(8-9), 747–755 (2007)
2. Wang, Y., Ajoku, P., Brustoloni, J., Nnaji, B.J.: Intellectual Property Protection in Collaborative Design through Lean Information Modeling and Sharing. Comput. Inf. Sci. Eng. 6, 149 (2006)
3. Cera, D.D., Kim, T., Han, J., Regli, W.C.: Role-based viewing envelopes for information protection in collaborative modeling. Computer-Aided Design 36(1), 873–886 (2004)
4. Fang, C., Peng, W., Ye, X., Zhang, S.: Multi-level access control for collaborative CAD. In: Proceedings of the Ninth International Conference on Computer Supported Cooperative Work in Design, vol. 1, pp. 643–648 (2005)
5. Pettifer, S., Marsh, J.: A Collaborative Access Model for Shared Virtual Environments. In: Proceedings of the 10th IEEE international Workshops on Enabling Technologies: infrastructure For Collaborative Enterprises. WETICE, pp. 257–262. IEEE Computer Society, Washington (2001)
6. Bullock, A., Benford, S.: An access control framework for multi-user collaborative environments. In: Proceedings of the international ACM SIGGROUP Conference on Supporting Group Work, pp. 140–149. ACM, NY (1999)
7. Walczak, K.: Structured Design of Interactive VR Applications. In: The 13th International Symposium on 3D Web Technology Web3D, Los Angeles, California, USA, pp. 105–113. ACM Press, NY (2008)
8. Latoschik, M.E., Biermann, P., Wachsmuth, I.: Knowledge in the Loop: Semantics Representation for Multimodal Simulative Environments. In: Butz, A., Fisher, B., Krüger, A., Olivier, P. (eds.) SG 2005. LNCS, vol. 3638, pp. 25–39. Springer, Heidelberg (2005)
9. Lugrin, J., Cavazza, M.: Making sense of virtual environments: action representation, grounding and common sense. In: Proceedings of the 12th international Conference on intelligent User interfaces, IUI 2007, pp. 225–234. ACM, NY (2007)
10. Pittarello, F., De Faveri, A.: Semantic description of 3D environments: a proposal based on web standards. In: Proceedings of the Eleventh international Conference on 3D Web Technology. Web3D 2006, pp. 85–95. ACM, NY (2006)

11. Gutierrez, M., Vexo, F., Thalmann, D.: Semantics-based representation of virtual environments. IJCAT 23, 229–238 (2005)
12. Sallés, E.J., Michael, J.B., Capps, M., McGregor, D., Kapolka, A.: Security of runtime extensible virtual environments. In: Proceedings of the 4th International Conference on Collaborative Virtual Environments, CVE 2002, pp. 97–104. ACM, NY (2002)
13. Tolone, W., Ahn, G., Pai, T., Hong, S.: Access control in collaborative systems. ACM Comput. Surv. 37(1), 29–41 (2005)
14. Izaki, K., Tanaka, K., Takizawa, M.: Authorization model based on object-oriented concept. In: Proceedings of the the 15th international Conference on information Networking. ICOIN, pp. 72–77. IEEE Computer Society, Washington (2001)
15. Wong, R.K.: RBAC support in object-oriented role databases. In: Proceedings of the Second ACM Workshop on Role-Based Access Control, Fairfax, Virginia, United States, RBAC 1997, pp. 109–120. ACM, New York (1997)
16. Sandhu, R., Ferraiolo, D., Kuhn, R.: The NIST model for role-based access control: towards a unified standard. In: Proceedings of the Fifth ACM Workshop on Role-Based Access Control, RBAC 2000, pp. 47–63. ACM, NY (2000)
17. Priebe, T., Dobmeier, W., Schläger, C., Kamprath, N.: Supporting Attribute-based Access Control in Authentication and Authorization Infrastructures with Ontologies. Journal of software: JSW 2(1), 27–38 (2007)
18. Wang, X., Demartini, T., Wragg, B., Paramasivam, M., Barlas, C.: The mpeg-21 rights expression language and rights data dictionary. IEEE Transactions on Multimedia 7(3), 408–417 (2005)
19. Moses, T. (ed.): eXtensible Access Control Markup Language (XACML) Version 2.0., http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf