A Foundation for Defining Security Requirements in Grid Computing

Antonios Gouglidis, Ioannis Mavridis
Department of Applied Informatics
University of Macedonia
Thessaloniki, Greece
agougl@uom.gr, mavridis@uom.gr

***Abstract*—Despite the wide adoption by the scientific community, grid technologies have not been given the appropriate attention by enterprises. This is merely due to the lack of enough studying and defining security requirements of grid computing systems. More specifically, access control in grid systems has been addressed with the same models for collaborative systems based on distributed computing across multiple administrative domains. However, existing solutions are not based on a foundation for a holistic approach in grid access control. This paper aims to provide an adequate approach in this direction. Additionally, a comparative review of current access control models is provided in the context of our proposed four-layer conceptual grid categorization.**

Access control; grid computing; security requirements engineering

I. INTRODUCTION

One of the emerging and prominent technologies in the recent years is grid computing. Grid computing technologies have been met with great acceptance from the scientific community. A large number of scientific experiments make use of grid technologies in order to tackle the enormous input of data, as well as the need for processing power to produce results. Such grid systems are, for example, Large Hadron Collider (LHC) [1] and SETI@home [2]. In parallel, an analysis started on how to fit existing business models into the grid in order for grid technologies to be adopted by the enterprises [3]. Business models refer to technologies such as utility computing and software as a service (SaaS). Due to some fundamental similarities between science and business grids, a significant number of requirements remain the same in both. Nevertheless, business grids require some enhancements in areas such as security [4]. To the best of our knowledge, the access control models used in current grid systems are not specifically designed for use in grid systems but instead, for general purpose and collaborative systems.

Motivated by the need for integrating business concepts into the grid and from the diverse requirements between science and business grid systems, we identify the need for a holistic approach in grid access control. The remainder of this paper is structured as follows: Section II provides a brief description of grid security issues. A conceptual categorization of grid systems is presented in section III. Section IV reviews access and usage control models used in grid systems and records a number of access control requirements in regard to the conceptual four-layer categorization. In section V a comparative review of access control models is presented and finally the paper is concluded in section VI.

II. GRID SECURITY ISSUES

Main security concepts met in grid systems, such as the ones identified in the existing literature [5]-[7] are presented in the rest of the section.

Confidentiality, integrity and availability are basic security requirements that also apply in grid systems. Confidentiality is mostly associated with encryption and provides information secrecy. Integrity offers protection from unauthorized modification of data. Availability assures that a system will provide its services when needed to a legitimate user. In a grid system, the former two are usually used in the authentication process of a user, and the latter refers mostly to the availability of grid services.

Non-repudiation is a security concept that provides guarantees between parties. In a hypothetical transaction between two users, non-repudiation assures that, in case the transaction has been successfully accomplished, none of them can deny that it occurred. This is extremely useful in enterprise environments where money transactions take place.

Trust is a complex security concept and a number of different definitions are surveyed in [8]. Trust relationships in a grid system add a lot of complexity due to their distributed nature. Trust management in grid environments includes trust negotiations, delegation of rights and revocations in a distributed manner and takes place in heterogeneous domains as well as between virtual organizations (VOs).

Authentication is the verification procedure of the identity of an entity in a system. In a grid system, there are a number of entities that have to be authenticated such as users, resources and services. One of the mechanisms used in authentication is the Public Key Infrastructure (PKI). However, PKI mechanisms seem to introduce a number of issues, like its adoption from users and administrative difficulties.

Authorization and access control are of vital importance in all systems, as in grids. Usually these two terms are confused. Authorization is the process of providing permissions on an authenticated user or service to access a specific resource. On the contrary, as defined in [9], access control's objective is to limit in a computer system the actions or operations performed directly by a legitimate user or by programs executed on behalf of a user. Further

information on grid authorization architectures can be found in [10].

III. A Conceptual Categorization of Grid Systems

Current grid systems have been categorized and classified in the existing literature based on different criteria, either qualitative or quantitative. It is an indisputable fact that most of these categorizations are quite vague, in regard to the limits of each category [11]. However, to the best of our knowledge, none of them provides a categorization by strictly considering the security issues raised in grid systems. Moreover, requirements' identification lacks an organized and structured model, able to enhance and facilitate the whole process. In order to provide a foundation for a holistic approach to grid's access control, we propose a conceptual four-layer categorization in order to identify the distinctive security requirements that are posed by each layer.

As depicted in Fig. 1, the proposed conceptual categorization of current grid systems is based on the following layers: entropy layer, assets layer, management layer and logic layer. The differentiation from existing approaches is that a number of factors affecting the security of grid systems are mainly taken into account in the proposed categorization. In brief, the conceptual categorization identifies and groups security requirements into discrete layers of different abstraction level. The abstraction level refers to each layer's ability to identify requirements in different breadth and depth. Therefore, the entropy layer depicts the system's expansion, while the assets layer what is shared within the boundaries defined by the entropy layer. The management layer poses requirements on how to manage assets within the limits of the system and finally the logic layer incorporates requirements that are not handled by the former layers.

A. Entropy Layer

Entropy is a layer capable of capturing the abstract characteristics of a system accrued from its distribution. The term entropy refers to the virtual and geographic spatial distribution of a system and the fluctuations of sharable resources in time. The homogeneous or heterogeneous resources can either be of hardware or software objects. Current classifications of grid systems are static and based mostly on the geographic distribution of their resources [12] or on their size [13]. The entropy layer couples existing grid distribution characteristics such as the ones described in the aforementioned literature, and extends them by considering quantitative factors such as their modification through time. Consequently, the entropy layer can describe a wide variety of systems, from small personal grid systems to greatly distributed peer-to-peer networks.

B. Assets Layer

The second layer is used to include all the assets of a grid system. As an asset we define a resource in a grid system that can be shared within a VO. In a grid system, an asset can either be of software or hardware type. The classification is partially based on the existing literature [12]-[15].

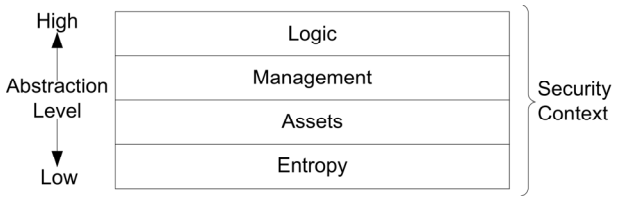

Figure 1. Conceptual grid categorization layers.

Under the software class, we further divide the assets into two subclasses, those of service and data. The provision of fine-grained assets, such as data, is vital in a grid system. We mention as an example the requirement of sharing information at data-record-level in a database management system among a number of users [5].

Similarly, we divide the hardware class into three subclasses, those of computational, storage and equipment. Examples of computational assets are the usage of CPU or RAM of a system. The storage assets, involve the usage of raw storage space for the saving of data. Last but not least, an equipment is an asset that is usually used as an input or output device within a grid system.

C. Management Layer

The management layer is used to fulfil the need for capturing the security issues raised from the management of policies between grid entities as well as trust relationships.

Based on the distribution level of a system, the policy management can either be centralized or de-centralized. Usually, systems with a low level of spatial distribution, as defined in the entropy layer, require a centralized management subsystem and vice-versa. A peer-to-peer network is an example that requires de-centralized management. On the contrary, a small local business application using grid technologies requires centralized management.

The enforcement of several management operations is another factor that needs to be further classified. Here we propose a two level enforcement solution, that of static and dynamic enforcement. By static we refer to operations that take place before and after the execution of a number of actions. The diversity of the dynamic enforcement of operations is that in the latter the enforcement can also take place during the execution of an action.

The automation level refers exclusively to the intervention of an administrator in the management routines. With fully automation, we mean management that is done by the grid system itself [16]. With semi automated systems, we particularize those that are partially managed by the system itself and the administrators. However, cases still exist where automation from the management routines is completely absent. Such systems are solely administered by humans. Operations such as problem identification, conflict resolution and revocation of privileges should be considered under this layer.

Ultimately, trust management must be taken under consideration in the security context of the grid. The life

cycle of trust includes the creation, negotiation and the management of it and is considered to be an important part in security [8].

D. Logic Layer

The last layer of logic, pertains to the application models and the type of their execution in a grid system. The proposed classification is based on the definition of grid systems, the requirements posed from the existing literature [3], [11] and topics that may raise security issues.

The logic layer is split into two classes. In the first abstract class of models, we try to capture the security issues that may rise from the nature of the application being executed in the grid. We propose a further classification into business and science applications. However, in both subclasses, similar requirements might exist. Usually the support of collaborations, workflows and co-operations fall under science projects. Nonetheless, in addition to the aforementioned, technologies such as software as a service (SaaS) and hardware as a service (HaaS) are required in business grid applications.

Based on the requirements of the applications executed in grid environments, we reckon their classification into batch and interactive. Usually, science projects require a batch-based execution of applications in order to provide results through the computation of data. In contrast, most business applications demand an interactive environment to tackle the highly dynamic enterprise environment.

IV. Access Control in Grid Systems

A. Current Approaches

Access control is a security concept of vital importance in all types of grid systems. In current grid systems, we can identify two main categories of access control models. The first is Role-Based Access Control (RBAC) [17] and the second is Usage Control (UCON) [18], [19]. The latter subsumes the Attribute-Based Access Control model (ABAC). To the best of our knowledge, there is no standard ABAC model [20], and hence we omit to further analyze it in the rest of this section.

RBAC is a proposed NIST standard [17]. The core model is composed of five static elements, viz users, roles and permissions, with the latter being composed of operations applied on objects. The relationship between the elements is quite straightforward. Roles are assigned to users and permissions are assigned to roles [21]. RBAC supports the principles of abstract privileges, least privilege, separation of administrative functions and separation of duties [22]. Recent research in [23] anticipates the enhancement of the RBAC model to a next-generation access control model by introducing the ASCAA principles. ASCAA stands for abstraction, separation, containment, automation and accountability. The principles of abstraction and separation remain the same as in the initial model. The least privilege principle is subsumed under containment and features such as usage and limits are introduced. Automation is added in order to tackle administration issues. Finally, accountability is introduced mainly to assign users with the responsibility of their actions being performed in a system. However, the application of the ASCAA principles in RBAC is currently under development. RBAC has proven its appropriateness and is used in a great number of enterprise systems, operating systems and databases. Despite its wide use, RBAC comprises a passive security system and for that reason a number of variant RBAC models exist [24]. A grid authorization system using RBAC is PERMIS [25].

UCON is a usage control model that has introduced a number of novelties in the way access control behaves. UCON's ABC model consists of eight components viz subjects, subject attributes, objects, object attributes, rights, authorizations, obligations and conditions [18]. The notion of subjects and objects as well as the usage of both subject and object attributes in UCON is quite straightforward. However, it is worth mentioning that the attributes can be mutable. Mutability is the one responsible for the update of subject and object attributes as a result of an access. The rights component is enabling access of subjects on objects. However, the determination of the right is done during the access operation and by considering the following decision factors: authorizations, obligations and conditions. Among other functionalities UCON supports continuity of decisions. This means that authorizations can occur before the access is allowed and during the access, until it ends. UCON is a new usage control system. Nevertheless, research has been done in [19] for its use in collaborative systems and has been adopted in GridTrust [26]. However, UCON as an ABAC model inherits its complexity and can be error-prone, especially in highly heterogeneous environments [27].

B. Four-layer Requirements Definition

In this section, a number of access control requirements identified in the literature are placed in the context of each one of the four layers presented in section III. The defined requirements are:

Entropy Requirement 1: The access control in a grid system must be done in a distributed manner. Both virtual and geographic distribution must be taken into consideration due to cross VO collaborations and geographically distributed domains. Thus, an access control system must limit access upon participating distributed entities.

Entropy Requirement 2: Each domain in a VO may be comprised of homogeneous resources. A VO is composed of multiple heterogeneous domains. Collaborations in a VO can be established between different domains of diverse resource types. The access control model must limit access to resources by overcoming their diverse characteristics.

Entropy Requirement 3: During the life of a VO, users or resources that belong to a domain can join in or quit of the collaboration. The access control system must tackle such modifications in the accompanied entities and enforce the required restrictions.

Assets Requirement 1: The resources in a VO can be of various types, from database row/column data to complex services and hosts. An access control model must be able to identify and cope with all types of resources, on different levels of access. Hence, the access control model must be granular and in position to apply both fine-grained and

coarse-grained access control policies [28]. Especially, in business grid systems, due to their wide range of applications, the support of both fine-grained and course-grained access control is of vital importance. For instance, fine-grained access at a data-record-level could be useful in database grid systems, where a possible use case of data replication might exist [5]. Likewise, course-grained access at a service-level could be useful in a SaaS scenario.

Management Requirement 1: In a VO new policies can be created by the resource stakeholders or a service provider. Moreover, it is possible for the policies to be modified during their lifetime in a session [28]. The access control model must be able to collect, compensate and enforce all distributed policies in a dynamic and deterministic way. By dynamic, we mean that the access control model must be in place to apply continuously any changes in the policies at any time during a session. By deterministic we mean that the access control model must be able to correctly produce the same output for a given start condition, and that it should be guaranteed to terminate [28].

Management Requirement 2: A grid access control model must be able to support trust relationships in a VO and provide functionalities such as distributed delegation of rights [28]. Delegated rights must permit further delegation if needed (re-delegation). Both delegated and re-delegated rights must be revoked on request or on time. The latter applies when delegation is used with constraints, such as time restrictions.

Management Requirement 3: A grid access control model must be able to support distributed policy conflict resolution. For example, let's assume that user A inherits authorization rights, to access resource R, from user B, which permits access to resource R, and user C, which denies access to resource R. If user A requests to access resource R, a conflict will occur, since user B permits access and user C denies access simultaneously on the same resource. The system must be able to resolve or avoid such conditions.

Management Requirement 4: All operations must be logged for security and traceability reasons.

Management Requirement 5: A grid access control model requires automation of procedures. Especially in business grid scenarios, requirements 1, 2, 3 and 4 must be done in an automated way to minimize human intervention and to increase the efficiency of the system [29].

Logic Requirement 1: Business grid systems require the support of interactive environments by the access control model [4], [29], [30]. The interactive environment demands a dynamic access control model, able to capture and enforce all the interactive changes during runtime.

Logic Requirement 2: Business grid systems require the support of stateful sessions by the access control model [29]. An access control model should be able to keep the state of the session until the completion of the operation. In business grids, cases exist in which the completion of an operation lasts long or business operations such as migration of components might occur.

Logic Requirement 3: An access control model must be able to handle the decomposition of composed services [31]. This requirement is vital, especially in business grids due to the extensive use of service-oriented architecture (SOA) technologies. The individual domains of a VO are able to provide services that can be composed and provided to a consumer as a composed service. By evaluating the individual service permissions, it is possible to permit or deny access on the requested resource.

V. A Comparative Review

The definition of grid access control requirements greatly enhances the identification of key features that must be supported by an access control model for grid systems. In addition, we further evaluate three basic access control models, that of ABAC, RBAC and UCON, in the context of our proposed four-layer conceptual categorization. The criteria used throughout the evaluation are the requirements posed in each one of the proposed layers.

In regard to the entropy layer, both ABAC and UCON, due to their support of attributes, can tackle highly distributed environments. Attribute repositories can be dispersed across different domains and attributes can easily be retrieved. The use of attributes also overcomes the heterogeneity problems in VOs. These two models are flexible enough to cope with dynamic modifications in the participating entities. On the contrary, RBAC seems to better handle centralized architectures where participants are known a priori.

Concerning assets, core RBAC is a coarse-grained instead of a fine-grained access control model. This is mainly because RBAC needs to group assets under roles. In order to support fine-grained access control, one assignment must be spilt into more, leading to their increment and thus becoming more rigid. Yet, enhanced RBAC models incorporate context variables to overcome such limitations. ABAC and UCON are able to handle fine-grained access control natively. Attributes can be as fine-grained as required.

RBAC supports improved administrative capabilities compared with the other two models. This is mainly because of user to role and role to permissions assignments. Revocation of user assignments can be easily supported. Role hierarchies, delegation and temporal constraints are more of RBAC's virtues. Trust can also be incorporated. However, RBAC lacks in topics such as distributed revocation, and distributed conflict resolution. ABAC and UCON can also incorporate trust mechanisms. Both handle distributed management better than RBAC, via distributed attribute repositories. In contrast to ABAC, UCON supports immediate attribute revocation. Nonetheless, conflict resolution can be cumbersome in both. UCON is the only among others that is able to dynamically enforce changes in policies. Automation is absent from all models.

Requirements in logic layer are handled poorly in overall by the examined models. However, UCON is capable of supporting interactive environments via continuity of decision and mutable attributes. Limitations on resources can be enforced through conditions and obligations can handle a number of business requirements. Still, topics like service composition are left intact.

Table I summarizes our evaluation on the different access control models.

VI. CONCLUSION

In this paper, motivated by the absence of a holistic approach in grid access control, we proposed a conceptual four-layer categorization of grid systems from a security perspective. The proposed categorization can facilitate the identification of access control requirements in grid systems due to its layered scheme. A demonstration in requirements identification was given. Furthermore, an evaluation of current access control models was provided in the context of the layered scheme. We expect the proposed categorization to be widely adopted in order to serve as a foundation for further defining access control requirements in grid computing and so resulting in new access control models for the grid environment.

TABLE I. EVALUATION OF ACCESS CONTROL MODELS

Access Control Models	**Conceptual Categorization Layers**			
	Entropy	***Assets***	***Management***	***Logic***
ABAC	High	Medium	Low/ Medium	Low
RBAC	Low/ Medium	Low/ Medium	Medium/ High	Low
UCON	High	Medium	Medium	Medium/ High

REFERENCES

[1] CERN. (2009, February) Large Hadron Collider (LHC) computing grid. [Online]. Available: http://public.web.cern.ch/public/en/LHC/Computing-en.html

[2] D. P. Anderson, J. Cobb, E. Korpela, M. Lebofsky, and D. Werthimer, "SETI@home: an experiment in public-resource computing," Commun. ACM, vol. 45, no. 11, pp. 56-61, November 2002.

[3] J. Altmann and D. Veit, Eds., Grid Economics and Business Models, 4th International Workshop, GECON 2007, Rennes, France, August 28, 2007, Proceedings, ser. Lecture Notes in Computer Science, vol. 4685. Springer, 2007.

[4] C. Franke, A. Hohl, P. Robinson, and B. Scheuermann, "On business grid demands and approaches," in GECON, 2007, pp. 124-135.

[5] P. J. Broadfoot and A. P. Martin, "A critical survey of grid security requirements and technologies," Oxford University Computing Laboratory, Tech. Rep. RR-03-15, August 2003.

[6] A. A. Marcim Adamski, P. F. Angelos Bilas, A. H. Vasil Georgiev, B. M. Gracjan Jankowski, J. P. Norbert Meyer, and M. Wilson. (2008, May) Trust and security in grids: A state of the art. CoreGRID, Network of Excellence.

[7] G. Angelis, S. Gritzalis, C. Lambrinoudakis, "Mechanisms for controlling access in the global grid environment", Internet Research, vol. 14, no. 5, pp. 347-352, Emerald, 2004

[8] A. Chakrabarti, Grid Computing Security, Managing Trust in the Grid. Springer Berlin Heidelberg, 2007.

[9] R. Sandhu and P. Samarati, "Access control: Principles and practice," IEEE Commun., vol. 32, no. 9, pp. 40-48, 1994.

[10] D. Chadwick, "Authorisation in grid computing," Information Security Technical Report, vol. 10, no. 1, pp. 33-40, 2005.

[11] S. W. Alexander Kipp, R. P. Lutz Schubert, C. T. Horst Schwichtenberg, and E. Karanastasis, "A new approach for classifying grids," BEinGRID, Tech. Rep., 2008.

[12] Gridipedia. (2009, February) Types of grid. Gridipedia. The European Grid Marketplace. [Online]. Available: http://www.gridipedia.eu/types-of-grids.html

[13] H. Kurdi, M. Li, and H. Al-Raweshidy, "A classification of emerging and traditional grid systems," IEEE Distributed Systems Online, vol. 9, no. 3, p. 1, 2008.

[14] D. Green. (2002, February) Grid technology. The future of the internet? the future of it? IBM Corporation. [Online]. Available: https://ludit.kuleuven.be/nieuws/pdf/grid.pdf

[15] M. M. Krauter K., Buyya R., "A taxonomy and survey of grid resource management systems for distributed computing," Softw. Pract. Exper., vol. 32, no. 2, pp. 135-164, 2002.

[16] J. Kephart, "Research challenges of autonomic computing," ACM, ICSE '05, pp. 15-22, May 2005.

[17] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chandramouli, "Proposed NIST standard for role-based access control," ACM Trans. Inf. Syst. Secur., vol. 4, no. 3, pp. 224-274, 2001.

[18] R. Sandhu and J. Park, "Usage control: A vision for next generation access control," Computer Network Security, pp. 17-31, 2003.

[19] X. Zhang, M. Nakae, M. J. Covington, and R. Sandhu, "Toward a usage-based security framework for collaborative computing systems," ACM Trans. Inf. Syst. Secur., vol. 11, no. 1, pp. 1-36, 2008.

[20] S. Busch, B. Muschall, G. Pernul, and T. Priebe, "Authrule: A generic rule-based authorization module," Springer Berlin Heidelberg, Data and Applications Security XX, LNCS, 2006

[21] D. F. Ferraiolo, D. R. Kuhn, and R. Chandramouli, Role-Based Access Control. Norwood, MA, USA: Artech House, Inc., 2003.

[22] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-based access control models," IEEE Computer, vol. 29, no. 2, pp. 38-47, 1996.

[23] R. Sandhu,V. Bhamidipati, "The ASCAA principles for next generation role-based access control," Proc. 3rd International Conference on Availability, Reliability and Security (ARES), Barcelona, Spain, March 4-7, pages xxvii-xxxii, 2008.

[24] W. Tolone, G.-J. Ahn, T. Pai, and S.-P. Hong, "Access control in collaborative systems," ACM Comput. Surv., vol. 37, no. 1, pp. 29-41, March 2005.

[25] D. W. Chadwick, A. Otenko, and E. Ball, "Role based access control with X.509 attribute certificates," IEEE Internet Computing, vol. 7, no. 2, pp. 62-69, 2003.

[26] GridTrust. (2009, February) Gridtrust. [Online]. Available: http://www.gridtrust.eu/gridtrust/

[27] T. Priebe, W. Dobmeier, and N. Kamprath, "Supporting attribute-based access control with ontologies," in ARES '06: Proceedings of the First International Conference on Availability, Reliability and Security. Washington, DC, USA: IEEE Computer Society, 2006, pp. 465-472.

[28] M. Humphrey, S.-M. Park, J. Feng, N. Beekwilder, G. Wasson, J. Hogg, B. LaMacchia, and B. Dillaway, "Fine-grained access control for gridftp using secpal," in GRID '07: Proceedings of the 8th IEEE/ACM International Conference on Grid Computing. Washington, DC, USA: IEEE Computer Society, 2007, pp. 217-225.

[29] R. Jimenez-Peris, M. Patino-Martinez, and B. Kemme, "Enterprise grids: Challenges ahead," J. Grid Comput., vol. 5, no. 3, pp. 283-294, 2007.

[30] A. Chakrabarti, Grid Computing Security, Grid Authorization Systems. Springer Berlin Heidelberg, 2007.

[31] E. Damiani, S. D. C. di Vimercati, and P. Samarati, "New paradigms for access control in open environments," in SIGNAL PROCESSING AND INFORMATION TECHNOLOGY, 2005, pp. 540-545.