Internet Research

A generic Grid security policy reconciliation framework

Lazaros Gymnopoulos, Vassilios Tsoumas, Ioannis Soupionis, Stefanos Gritzalis,

A generic Grid security policy reconciliation framework

Lazaros Gymnopoulos
ICSS Laboratory, University of the Aegean, Samos, Greece
Vassilios Tsoumas and Ioannis Soupionis
ISDB Laboratory, Athens University of Economics and Business, Athens, Greece, and
Stefanos Gritzalis
ICSS Laboratory, University of the Aegean, Samos, Greece

Abstract

Purpose – The purpose of this paper is to provide a framework for enhancing security policy management in the Grid.

Design/methodology/approach – The Grid security policy reconciliation problem is presented. A generic view on the security policy notion is adopted and the security policy ontology notion is introduced and used.

Findings – In the course of this work it was found that, in order to enhance security policy management in the Grid, Grid entities should have the ability to negotiate their security policies. It was also found that, in order to achieve security policy negotiation, effective security policy semantics manipulation towards security policy reconciliation is needed. Finally, it was established, through the use of an example, that if appropriate means are used for security policy reconciliation then incompatible security policy representations can be transformed into compatible ones.

Research limitations/implications – Research limitations stem from the adoption of a generic view on the security policy notion and the selection of identification and authentication security policies as the focal point of the proposed framework. Research implications include the possibility of examining how existing security policy reconciliation models can be incorporated in this generic framework. The possibility of investigating how such a framework can lead to a security policy knowledge management tool for Grid administrators is also demonstrated.

Practical implications – Practical implications of this work include the establishment of a common framework for security information exchange between Grid entities.

Originality/value – This paper proposes a framework for enhancing security policy management in the Grid. The proposed framework can be used by researchers as a reference and by security experts in order to reduce ambiguity concerning the interpretation of security policies expressed in different forms, by negotiating Grid entities.

Keywords Data security, Conflict resolution, Business policy

Paper type Research paper

1. Introduction

Information systems are evolving from static, geographically confined and isolated “information islands” to dynamically formed, geographically dispersed “information spaces” that are fully interconnected; such “information spaces” are usually referred to as virtual organizations (VOs) (Foster *et al.*, 2001). The Grid infrastructure (Foster *et al.*, 2005) is a major step towards achieving coordinated resource sharing and problem solving within and among VOs. In order to achieve these goals, the Grid manages

Internet Research
Vol. 15 No. 5, 2005
pp. 508-517
© Emerald Group Publishing Limited
1066-2243
DOI 10.1108/10662240510629457

intrinsic complexity by defining various abstraction layers, namely fabric, connectivity, resource, collective, and application layers (Foster *et al.*, 2001).

Security management and configuration takes place throughout these layers, and thus complicates the job of security administrators. In the lower Grid layers security interfaces exist between local systems and the Grid (local security policies against global security policies). Matching local security policies to Grid security policies poses an important security challenge. While existing security policy conflict resolution or reconciliation frameworks have been applied within specific Grid architecture layers (Wang *et al.*, 2004) – with emphasis being given to the lower, more concrete ones – little attention has been given to generic security policy reconciliation frameworks. Such a framework could address the security policy management problem throughout Grid abstraction layers, from the more concrete to the more abstract ones.

Before introducing our proposed security policy reconciliation framework, we present in the following section an overview of Grid security challenges and requirements, accentuating the generic perspective of the Grid security policy reconciliation problem. In Section 3, we make clear that security policy is a multi-interpreted notion and that various ways exist for representing security policies. We base upon this diversity in order to define the fundamental attributes of our framework: manipulation of security policy semantics towards compatible representation of security policies. In Section 4, we analyze the security policy ontology (SPO) notion and provide some basic SPO design criteria. In Section 5, we present a high-level, generic framework for the enhancement of security policy management in the Grid. Finally, in Section 6 we conclude and present future work proposals along with unresolved research issues.

The main contributions of this paper are:

- the provision of a generic security policy reconciliation framework that can be used in order to enhance security policy management in the Grid;
- the establishment of the potentiality to transform incompatible security policy representations into compatible ones; and
- the clarification of the Grid security policy reconciliation problem.

2. The Grid security policy reconciliation problem

As a revolutionary technology, the Grid poses new security concerns, not so much in terms of the appearance of novice threats but in terms of the need for increased intensity and flexibility of security mechanisms (Jackson *et al.*, 2001). In this perspective one can argue that although the Grid incorporates known security challenges and requirements it also introduces some new ones.

An overview of those challenges and requirements is presented in Gymnopoulos *et al.* (2003). In general, security challenges in the Grid can be classified in three categories: integration with existing security architectures and models implemented across platforms and hosting environments, interoperability of multiple domains and hosting environments at protocol, policy and identity level, and establishment of trust relationships among the participants in a Grid system. Meeting the above-mentioned security challenges, and thus effectively managing and configuring security, is a much tougher problem in the Grid than it is in classic distributed computing. This is due mainly to three characteristics of Grid computing: dynamic environment, autonomy and common goal.

First, the formation of a VO is an entirely dynamic procedure. New resources may become available for sharing at any given time (e.g. if redeemed from another computation) just as new computational needs may occur (e.g. intense need for CPU cycles during a large scale simulation). Second, the lack of central control allows each entity to pursue its own security objectives. Thus, the security problem is upgraded from protecting "the good from the bad" to "reconciling different security perspectives". Finally, despite the absence of central control, coordinated sharing and problem solving is still a Grid objective. Thus, the advanced security manipulation described above must be, in the general case, consistent with the need for specific qualities of service (QoS).

The above analysis indicates that generic security policy reconciliation models are vital for managing security in the Grid. Indeed, if a generic framework is applied that reduces ambiguous interpretation of heterogeneous security policies between negotiating Grid entities then both autonomy and a dynamic environment can be achieved easier. Especially, the need for specific QoS indicates that such a framework should, in the general case, impose the slightest possible load on Grid transactions.

3. Security policy representation

As Wang *et al.* (2004) note, "The term 'security policy' has come to mean different things to different communities". Indeed, the term "security policy" is interpreted in entirely different ways that vary from the practical view of a "vital, direction giving document" (Höne and Eloff, 2002) to the formalistic definition: "a security policy is a statement of what is, and what is not, allowed" (Bishop, 2002) and from the systemic approach presented in Kokolakis and Kiountouzis (2000) to the systematic definition given in McDaniel and Prakash (2002).

The existence of various interpretations is rooted in two facts. Firstly, security policy is a context dependent notion (e.g. computer security policy, information security policy, etc.) and secondly, even in the same context specific kinds of security policies have been developed to meet specific needs (e.g. confidentiality security policies in military environments, etc.). Both facts are indicative of the abounding, in terms of semantics, environment that security policies exist in. Therefore, in order to manage multiple interacting security policies – and that is the case of the Grid – one has to manage their semantics first.

Along with various interpretations of the security policy notion, several methods of security policy representation also exist. Suggestively we mention two polar views that adopt different scientific paradigms. As mentioned above, Kokolakis and Kiountouzis (2000) adopt the systemic paradigm in order to construct a "Metapolicy Development System", while, on the other side, Gong and Qian (1994) adopt the systematic paradigm and propose axiomatic rules for the synthesis of security policies such as the "principle of autonomy" and the "principle of security". Beyond the above-mentioned approaches several more exist and can be roughly divided in the following categories: verbal descriptions (Höne and Eloff, 2002), modeling (Bishop, 2002), specification (Damianou *et al.*, 2001), and formalization (Bishop, 2002; Trcek, 2000).

The existence of a large number of representation methods leads to the conclusion that security policies, even when being semantically compliant, can be presented in ways that differ substantially in terms of formalism, structure, and hierarchy thus raising obstacles in their reconciliation. Therefore, in order to effectively manage security policies one has to be able to produce compatible policy representations.

4. Security policy ontologies

In the previous paragraph we demonstrated the need to manipulate security policy semantics. An efficient means for achieving this purpose is ontology. Ontology is "an explicit specification of a conceptualization" (Gruber, 1993). Domain-specific ontologies are used to define the terminology for a group of people that share a common view on a specific domain (Decker *et al.*, 1999), effectively supporting knowledge sharing and reuse. Thus, security policies can be represented by the means of a SPO, which elaborates on the domain of security knowledge. SPOs can be used to describe structurally heterogeneous security policies of different levels of abstraction. Thus, by defining shared and common domain theories and vocabularies, SPOs help both people and machines to communicate in a concise manner, a manner which is based not only on the syntax of security policy statements, but on their semantics, as well.

Hereby we present the basic SPO design criteria extending definitions from Gruber (1993), in order to adapt to the security policy domain:

- *Clarity.* An SPO should effectively communicate the intended meaning of defined terms. Definitions should be expressed in an objective manner. While the motivation for defining a concept might arise from social situations or computational requirements, the definition should be independent of any social or computational context.
- *Coherence.* An SPO should be coherent; that is, it should attest inferences that are consistent with the security definitions. At least, coherence should apply to the defining axioms.
- *Extendibility.* An SPO should offer a conceptual foundation for a range of anticipated tasks, and the representation should be crafted so that one can extend and specialize the ontology *monotonically*.
- *Minimal encoding bias.* An encoding bias occurs when representation choices are made purely for the convenience of notation or implementation. Encoding bias should be minimized, because knowledge-sharing entities may be implemented in different representation systems and styles of representation.
- *Minimal ontological commitment.* An SPO should make as few claims as possible about the world being modeled, allowing the parties committed to the ontology freedom to specialize and instantiate the ontology as needed (with the exception of compliance to legal requirements, such as Data Privacy Acts in place).

5. A framework for enhancing security policy management in the Grid

In Section 3, we made clear that security policy is a multi-interpreted notion and that various ways exist for representing security policies. Two conclusions were drawn:

(1) one has to deal with security policy semantics first in order to achieve effective reconciliation of security policies in the Grid; and

(2) compatible representations of security policies are also considered a prerequisite for effective reconciliation of security policies in the Grid.

In Figure 1 we show a basic architectural design for a high-level framework that enhances security policy management in the Grid. The proposed framework incorporates both previously drawn conclusions. In order to achieve effective management and homogenization of policy semantics we use a SPO builder. In order to

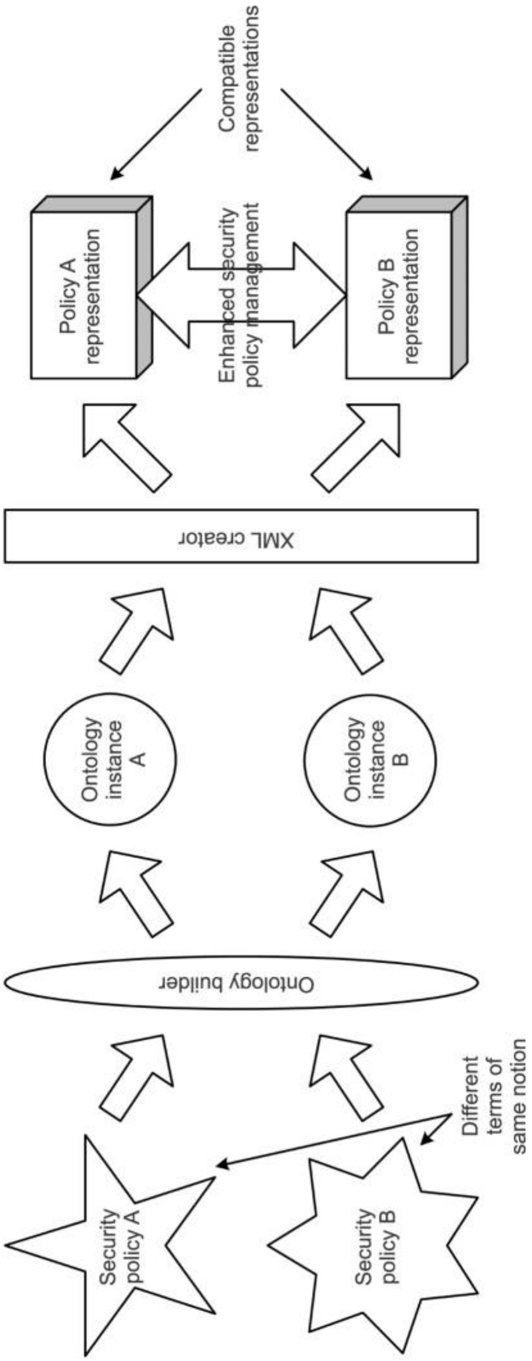

Figure 1.
A framework for enhancing security policy management in the Grid

achieve representation compatibility we use an XML creator. The framework produces compatible representations of security policies that were originally represented in incompatible formats. Therefore, the reconciliation and consequently the management of security policies become easier.

In particular, we assume Grid entities (e.g. a resource provider and a resource requestor) that have distinct security policies (security policies A and B, respectively, in Figure 1) possibly expressed in different languages or even representation models. Both policies are fed into the ontology builder (shown as an oval in Figure 1). The builder produces a single ontology representation that incorporates notions that appear in both policies. Each security policy, along with the respective representation model, is then described by a corresponding instance of the aforementioned SPO (ontology instance A and B, respectively, in Figure 1). The two ontology instances are then used by an XML creator (shown as a rectangle in Figure 1) in order to acquire the basic concepts along with their properties and transform them into XML tags and values (policies A and B representation, respectively, in Figure 1).

At this point we have to clarify the two basic elements of our framework.

First, we note that the ontology builder is a semi-automated process that can scan security policy representations and extract security related notions along with their properties and respective values. The builder uses appropriate interfaces in order to handle the existing plethora of different policy representations. For example, since most security policy representations follow XML standards, this extraction task can be realized using tools that follow the XML family of standards (e.g. XQuery, XSLT). The acquired notions can then be used for the construction of ontologies which can in turn be merged using one of various existing techniques (Kotis and Vouros, 2004). As an outcome, the ontology builder process constructs several instances of a single SPO that reflect the initial security policies. In this way security policy semantics homogenization is achieved.

Second, the XML creator refers to an automated system that is capable of transforming ontology concepts into XML tags and at the same time infuses the proper values to respective attributes. It is noted that the creator's ability to produce compatible security policy representations is partially based on the fact that it is fed with data by two instances of the same ontology.

5.1 Example usage of the proposed framework

In order to clarify the previously presented framework we provide an example concerning two simple Grid security policies. We assume a simple VO, namely VO A, and a user that wishes to become a member of A and consequently access its resources. VO A and the user have distinct security policies that are represented in arbitrary formats. Here we present both policies in natural language (Table I).

Each policy regardless of the representation method incorporates some basic security notions along with their attributes. The ontology builder discussed in the previous section has the ability to identify those notions and attributes and successively combine them into a single ontology as shown in Table II. Some notions, as, for example, "ID" from the VO security policy and "Identification token" from user security policy, are identified as identical and merged. Others, such as "Resource", exist only in one policy (the VO policy in our example) and are therefore carried over. It should be noted, that the structure of each policy is notably different and thus in the general case the ontology builder also has ability to shift a notion from one ontology level to the other.

User security policy		
Authentication	Authorization	Privacy
User owns a valid pair of identification token and password		
User is provided with a Kerberos ticket	User is member of either group: "Administrator" or "Restricted"	Network configuration data are not allowed to be transmitted
VO security policy		
Authentication	Authorization	Logging
Each entity (user or process) that wishes to use a resource must have:		
A valid pair of ID and password A valid X.509 certificate The X.509 certificate must be of a limited duration	Each entity that uses resources must have: A valid pair of ID and password	
Each resource must have: A valid X.509 certificate The X.509 certificate must be of an extended duration	Each entity that uses resources that belong to group "privilege" must have: A valid pair of ID and password Belong to the group "privileged"	For each access to the resource the following data should be logged ID, password, and IP address of the entity that used the resource

Table I.
An example of user security policy and an example of VO security policy

Ontology builder outcome	User security policy	VO security policy
Entity	Null	Entity
Type {User‖Process}	Null	Type
Identifier	Identification token	ID
Password	Password	Password
Certificate	Ticket	Certificate
Type {Kerberos‖X.509}	Type	Type
Duration {Extended‖Limited}	Null	Duration
Group {Administrator‖Restricted}	Group	Group
Net configuration	Net configuration data	Null
IP	Null	IP
Allowed {YES‖NO}	Allowed	Null
Resource	Null	Resource
Group {Privilege‖No Privilege}	Null	Group
Certificate	Null	Certificate
Type {Kerberos‖X.509}	Null	Type
Duration {Extended‖Limited}	Null	Duration

Table II.
Ontology builder produces coherent security policy ontologies

Finally, the ontology builder produces two instances of the same ontology one for each policy. The XML creator is then used to transform the ontology instances into compatible XML representations in order to facilitate automatic security policy management. Table III depicts the compatible security policy representations produced by the framework.

6. Conclusions and further research

In this paper, we outlined a framework for the enhancement of security policy management in the Grid. At present the proposed framework focuses on identification

User security policy	VO security policy
<?xml version="1.0" encoding="ISO-8859-1" ?>	<?xml version="1.0" encoding="ISO-8859-1" ?>
< Final_Policy >	< Final_Policy >
< Entity >	< Entity >
< Type/>	< Type > User </Type >
< Identifier > UserId </Identifier >	< Identifier > UserId </Identifier >
< Password > UserPassword </Password >	< Password > UserPassword </Password >
< Certificate >	< Certificate >
< Type > Kerberos </Type >	< Type > X.509 </Type >
< Duration/>	< Duration > Limited </Duration >
< /Certificate >	< /Certificate >
< Group > Restricted </Group >	< Group > </Group >
< Net_Configuration >	< Net_Configuration >
< IP/>	< IP > UserIP </IP >
< Allowed > NO </Allowed >	< Allowed/>
< /Net_Configuration >	< /Net_Configuration >
< /Entity >	< /Entity >
< Resource >	< Resource >
< Group/>	< Group > Privilege </Group >
< Certificate >	< Certificate >
< Type/>	< Type > X.509 </Type >
< Duration/>	< Duration > Extended </Duration >
< /Certificate >	< /Certificate >
< /Resource >	< /Resource >
</Final_Policy >	</Final_Policy >

Table III. The framework produces compatible security policy representations

and authentication security policies. We argued that our framework can contribute to the reduction of ambiguity concerning the interpretation of security policies expressed in different ways between negotiating Grid entities. The establishment of a common framework for security information exchange between Grid parties also provides the foundations for enforcing, evaluating and auditing the security level of the Grid security function in a uniform way. Moreover, such a framework supports comparable and reusable axioms between security policies, thus providing a means for semantic queries against a Grid policy base.

In this perspective and besides implementing and testing our framework other open issues exist. For example, the way existing security policy reconciliation models can be incorporated into a generic framework, both in the general case and in specific examples, could be examined. Furthermore, an analytical mapping of the proposed framework with Grid architecture layers should be provided. Finally, we plan to investigate how such a framework can be used in order to produce a security policy knowledge management tool for administrators in the Grid.

References

Bishop, M. (2002), *Computer Security: Art and Science*, Addison-Wesley, New York, NY.

Damianou, N., Dulay, N., Lupu, E. and Sloman, M. (2001), "The ponder policy specification language", in Sloman, M., Lobo, J. and Lupu, E.C. (Eds), *Proceedings of the International Workshop on Policies for Distributed Systems and Networks*, Springer-Verlag, Bristol, pp. 18-38.

Decker, S., Erdmann, M., Fensel, D. and Studer, R. (1999), "Ontobroker: ontology based access to distributed and semi-structured information", in Meersman, R., Tari, Z. and Stevens, S.M. (Eds), *Proceedings of DS-8: Semantic Issues in Multimedia Systems*, Kluwer Academic Publishers, Dordrecht, pp. 351-69.

Foster, I., Kesselman, C. and Tuecke, S. (2001), "The anatomy of the grid: enabling scalable virtual organizations", *International Journal of High Performance Computing Applications*, Vol. 15 No. 3, pp. 200-22.

Foster, I., Kishimoto, H., Savva, A., Berry, D., Djaoui, A., Grimshaw, A., Horn, B., Maciel, F., Siebenlist, F., Subramaniam, R., Treadwell, J. and Von Reich, J. (2005), "The open grid services architecture, version 1.0", Global Grid Forum document, available at: www.ggf.org/documents/GFD.30.pdf (accessed 28 July 2005).

Gong, L. and Qian, X. (1994), "The complexity and composability of secure interoperation", *Proceedings of the 1994 IEEE Symposium on Security and Privacy*, IEEE Computer Society Press, Oakland, CA, pp. 190-200.

Gruber, T.R. (1993), "Toward principles for the design of ontologies used for knowledge sharing", *International Journal of Human-Computer Studies*, Vol. 43 No. 5, pp. 907-28.

Gymnopoulos, L., Dritsas, S., Gritzalis, S. and Lambrinoudakis, C. (2003), "Grid security review", *Lecture Notes in Computer Science*, Vol. 2772, pp. 100-11.

Höne, K. and Eloff, J.H.P. (2002), "Information security policy: what do international information security standards say?", *Computers & Security*, Vol. 21 No. 5, pp. 402-9.

Jackson, K.R., Johnston, W.E. and Talwar, S. (2001), "Overview of security considerations for computational and data grids", in Bashor, J. (Ed.), *Proceedings of the 10th IEEE International Symposium on High Performance Distributed Computing (HPDC-10 '01)*, IEEE Computer Society Press, San Francisco, CA, pp. 439-40.

Kokolakis, S.A. and Kiountouzis, E.A. (2000), "Achieving interoperability in a multiple-security-policies environment", *Computers & Security*, Vol. 19 No. 3, pp. 267-81.

Kotis, K. and Vouros, G.A. (2004), "The HCONE approach to ontology merging", in Bussler, C., Davies, J., Fensel, D. and Studer, R. (Eds), *Proceedings of the 1st European Semantic Web Symposium*, Springer-Verlag, Heraklion, pp. 137-51.

McDaniel, P. and Prakash, A. (2002), "Methods and limitations of security policy reconciliation", *Proceedings of the 2002 IEEE Symposium on Security and Privacy*, IEEE Computer Society Press, Oakland, CA, pp. 73-87.

Trcek, D. (2000), "Security policy conceptual modeling and formalization for networked information systems", *Computer Communications*, Vol. 23 No. 12, pp. 1716-23.

Wang, H., Jha, S., Livny, M. and McDaniel, P.D. (2004), "Security policy reconciliation in distributed computing environments", in Chadha, R. (Ed.), *Proceedings of the 5th IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'04)*, IEEE Computer Society Press, Yorktown Heights, NY, p. 137.

(Lazaros Gymnopoulos was born in Thessaloniki, Greece in 1975. He holds a Diploma in Electrical and Computer Engineering from the Aristotle University of Thessaloniki (AUTH) and an MSc in Information Systems from the Athens University of Economics and Business (AUEB). Currently, he is pursuing a PhD in Information and Communication Systems Security at the University of the Aegean, School of Sciences, Department of Information and Communication Systems Engineering, Samos, Greece. His e-mail address is lazaros.gymnopoulos@aegean.gr

Vassilios Tsoumas holds a Diploma in Informatics and an MSc in Information Systems from the Athens University of Economics and Business (AUEB). He also holds CISSP, CISA and CISM certifications. Currently, he is pursuing a PhD in Information Systems Security Management at the Athens University of Economics and Business (AUEB), Department of Informatics, Athens, Greece. His e-mail address is bts@aueb.gr

Ioannis Soupionis was born in Athens, Greece in 1980. He holds a Diploma in Informatics and Telecommunications from the National and Kapodistrian University of Athens (UoA) and an MSc in Information Systems from the Athens University of Economics and Business (AUEB). His e-mail address is jsoup@aueb.gr

Stefanos Gritzalis holds a BSc in Physics, an MSc in Electronic Automation, and a PhD in Informatics all from the National and Kapodistrian University of Athens (UoA). Currently, he is an Associate Professor, the Head of the Department of Information and Communication Systems Engineering, and the Director of the Laboratory of Information and Communication Systems Security (Info-Sec-Lab) at the University of the Aegean, School of Sciences, Samos, Greece. His e-mail address is sgritz@aegean.gr)