Towards Providing Security as a Service for Grid-Based Infrastructures

E. K. Olatunji, E. Jembere, M.O. Adigun
Department of Computer Science, University of Zululand
Private Bag X1001, KwaDlangezwa, 3886
Tel: +27 (0)35 902 6012, +27 (0)35 902 6189
email: aekolatunji05@yahoo.com,ejembere@yahoo.co.uk, madigun@pan.uz.ac.za

Abstract - A large scale service-oriented computing like grid presents several unique and challenging security issues that are not addressed by traditional client-server / distributed environment, especially with respect to authentication and authorization. The currently existing authentication and authorization frameworks for client-server distributed systems are not satisfactory in meeting the access requirements of a grid environment. Such requirements include the need to have support for multiple authentication and authorization mechanisms. This research work proposes a security framework that will provide the higher-level security functions of authentication and authorization as reusable services for grid-based infrastructures. The proposed security-as-a-service (SecaaS) framework will have support for multiple mechanisms for authentication and authorization, so that grid entities (services, resources, service requestors and service providers) can freely subscribe to their preferred mechanism for authentication and/or authorization. This research will involve in-depth literature survey, prototype implementation of the SecaaS architecture and evaluation of the framework through simulation experiments.

Index Terms — **Authentication, Authorization, Distributed Systems, Grid, Security.**

I. INTRODUCTION

A Grid can be described as consisting of collaboration of distributed(networked) computers pooling their resources together in a coordinated manner to enable users to utilize processing, storage, software, and data resources from any of the interconnected computers, leading to a greater resource sharing and higher utilization. [1].

Security, however, is a big challenge in distributed systems, as it involves the federation of multiple heterogeneous, geographically dispersed autonomous administrative domains. A large scale service-oriented computing like grid presents several unique and challenging security issues that are not addressed by traditional client-server distributed environment [2, 3], and this inhibits its wide adoption despite its many benefits. Such challenges include: the need to support multiple authentication mechanisms, single sign- on, dynamic delegation of access rights; support for multiple access control models, etc.

There has been continuous efforts in the development of authentication and authorization infrastructures to address the security challenges of grid environments [3, 4, 5]. However, none of this has been able to adequately satisfy the access requirements of distributed services [2, 3].

The access requirements of distributed services depend on many factors such as privacy requirements of the requester, authentication requirements of the service, trust relationship with the requester, authorization management policies among participating parties [2, 6]. The security of a grid system should be able to provide the same protection that conventional systems provide, including authentication , secure communication, authorization, and auditing [2]. In addition, the security infrastructure for grid and web services must be able to support more advanced security features like dynamic delegation of access rights, single sign-on / sign-off, dynamic establishment of trust relationship among multiple domain, privacy and policy related security issues in a federated environment [6]. Furthermore, the authorization mechanism of grid computing platform, for example , needs to support multiple security policies and have flexibility to support dynamism in security policies [2].

Realization of the inadequacy of existing security infrastructures for distributed environments to support a grid system has led to the development of a number of authentication and authorization infrastructures and models, most of which are application or domain specific. This approach of providing domain-specific security infrastructure is a duplication of effort, resulting in increased cost in application development and maintenance. This research effort is being attempted in the belief that a better approach to addressing security issues in a grid environment will be to develop a security framework that will provide security functions that satisfy access requirements of applications in grid environments as reusable services that can be subscribed to. In this way, developers will be able to concentrate on the application logic and at the same time be able to weave a centralized security infrastructure into their applications

II. RELATED WORK

Literatures abound with a lot of research efforts that have been carried out to address security issues in a large distributed environment like grid. Singh, Singh & Kaur [7] and Jie et al [3] reviewed a number of projects and models that have been carried out in an effort to address authorization and access control related issues in one form or the other.

Security infrastructures/technologies like Globus GSI, Kerberos, and Athens are common authentication infrastructures for grid systems. However, each of them makes use of only one mechanism for authentication; none has support for multiple authentication mechanisms. Kerberos is not explicit in provision of single sign-on feature, while Athens has no support for delegation. Support

for these features are desirable in grid security infrastructures[3, 5] . In the same vein, authorization infrastructures like CAS, VOMS, PERMIS and Akenti have provision for only one authorization model, using either user name, a user group, a user role, user attribute, etc. Ideally, service providers only need to determine what type of access to grant to different categories of users and then leave the authorization infrastructure to enforce the policies [3].

A number of researchers have also observed the inadequacy of many of the existing security infrastructures to satisfy the authentication and access requirements of distributed services and have been motivated to propose, design and implement other authentication and/or authorization frameworks and models for distributed services [2, 5, 6 7, 8]. However, these frameworks are mostly domain or application-specific. This is a duplication of effort, that will lead to increase in the cost of developing and maintaining applications. Furthermore, none of the models proposed by these scholars has provision for multiple mechanisms in carrying out these basic security functions. This work intends to address this gap.

III. PROPOSED RESEARCH APPROACH

In this work, the proposed Security as a Service (SecaaS) framework will focus on security functions related to authentication and authorization. The reference architecture of the proposed SecaaS framework is as shown in Figure 1. The reference architecture is based on the understanding that the actual process of gaining access to a protected resource / service begins with identification, followed by authentication and then by authorization. Both the authentication and authorization components of SecaaS will be designed to support variety of mechanisms for their operations. Fine-grained authorization will also be supported.

This research will employ literature survey to enable us investigate, analyze and evaluate how and why existing security frameworks for distributed environment fail to satisfy necessary access control requirements of distributed web services. The outcome of the literature survey will assist us in formulating an appropriate approach to implementing the reference model of our proposed SecaaS framework.

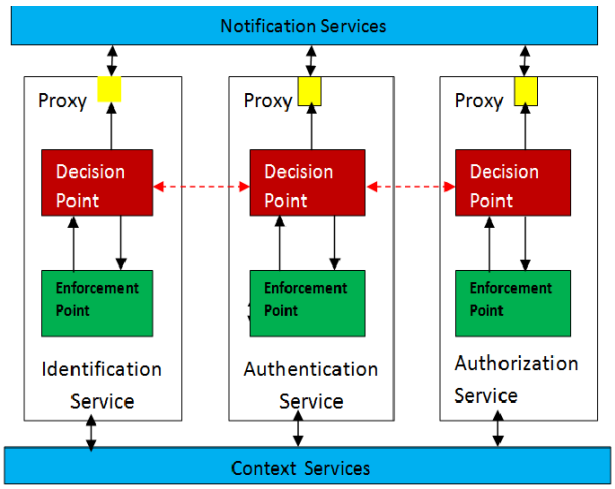

Figure 1. Reference Architecture of SecaaS Model

After prototyping the SecaaS framework, simulation experiment will be carried out to evaluate the effectiveness and performance of the resulting security framework.

IV. CONCLUSION

A Security as a Service framework aimed at providing higher-level security services of authentication and authorization for grid-based infrastructures has been proposed in this work in progress. The SecaaS framework will be designed to support mechanisms for authentication and authorization so as to give grid entities the liberty and flexibility to specify their preferred mechanisms. This approach will minimize duplication of efforts and costs in developing and maintaining different security frameworks. Changes to security requirements will only entail modifying the policies, without requiring changes to the application or access control and/or authentication mechanisms.

V. ACKNOWLEDGMENT

The authors are grateful to the Head and Management of the Centre of Excellence, Telkom / Huawei and the Department of Computer Science, University of Zululand, for supporting this research proposal.

VI. REFERENCES

[1] Ekabua, O.O (2009), Change Impact Analysis Model-Based framework for Service Provisioning in a Grid Environment, Ph.D Thesis Dept of Computer Science, UniZulu, RSA.

[2] Ekabua,O.O & Adigun M.O. (2010) GUISET LogOn: Design and Implementation of GUISET-driven Authorization framework, IARIA

[3] Jie, W., Arshad, J., Sinnott, R., Townend, P & Lei, Z. (2011),A Review of Grid Authentication and Authorization Technologies and Support for Federated Access Control, ACM Computing Survey, vol.43, no 2, Article 12, January 2011.

[4] Bertino, E; Martino, L.D; Paci, F. & Squicciarini, A.C (2010), Security for Web Services and Service-Oriented Architecture, London, Springer.

[5] Singh, S., Singh, K., & Kaur, H. (2009), Design and Evaluation of policy-based Authorization Model for large Scale Distributed Systems, IJCSNS International Journal of Computer Science and Network Security, Vol. 9 No. 11, pg 49-55

[6] Singh,S. & Bawa,S. (2007), A Privacy, Trust and Policy based Authorization Framework for services in Distributed Environment, International Journal of Computer Science,Vol 2 , No. 2.

[7] Squicciarini, A.C., Bhargav-Spantzel, A.,Bertino E., & Czeksis, A.B. (2007), Auth-SL – A System for the Specification Enforcement of Quality-Based Authentication policies, ICICS, pg 386-397.

[8] Lang, B.O ,Foster ,I., siebenlist, F .,Ananthakrishnan, R.,& Freeman,T. ((2008). A Multipolicy Authorization Framework for Grid Security. http://www.mcs.anl.gov/uploads/cels/papers, Retrieved on 23-05-2011.

Ezekiel Olatunji is a Ph.D student at the Department of Computer Science, University of Zululand. His research interest includes security for grid systems and web services.