SECURITY ISSUES IN GRID COMPUTING

Neha Mishra[1], Ritu Yadav[2] and Saurabh Maheshwari [3]

Department of CSE, Govt. Women Engineering College, Ajmer, Rajasthan, India

ABSTRACT

Grid computing is concerned with the sharing and use of resources in dynamic distributed virtual organizations. The dynamic nature of Grid environments introduces challenging security concerns that demand new technical approaches. In this brief overview we review key Grid security issues and outline the technologies that are being developed to address those issues. We focus on works done by Globus Toolkits to provide security and also we will discuss about the cyber security in Grid.

KEYWORDS

Virtual Organisation (VO), X.509,OSGA, GSI, CAS,WSDL, SSH.

1. INTRODUCTION

Security is a latest topic today for the smart grid, and progresses are being done in this field every day. Most communications uses standard cryptographic algorithms AES-128 to protect the data on the network. Grid computing is a technique which provides high-performance computing; in this resources are shared in order to improve the performance of the system at a lower price. According to literature, "Grid computing is a system where multiple applications can integrate and use their resource efficiently".

According to Foster and Kesselman, "A grid is a system that has three important categories: coordination of resources not under centralized control, use standard general purpose interface, and it delivers nontrivial quality of service". Kon et al define grid computing as, "coordination of resource sharing and dynamic problem solving in multi-institution virtual organizations" [3].

2. SECURITY REQUIREMENTS

Grid systems and applications require standard security functions which are authentication, access control, integrity, privacy, and no repudiation. Authentication and access control issues are. It (1) provide authentication to verify the users, process which have user's computation and resources used by the processes to authenticate (2) allow local access control mechanisms to be used without change. To develop security architecture we have to satisfy the following constraints which are taken from the characteristics of grid environment and application [1].

Single sign-on: A user should authenticate once and they should be able to acquire resources, use them, and release them and to communicate internally without any further authentication.

Protection of credentials: User passwords, private keys, etc. should be protected.

Interoperability with local security solutions: Access to local resources should have local security policy at a local level. Despite of modifying every local resource there is an interdomain security server for providing security to local resource.

Exportability: The code should be exportable i.e. they cannot use a large amount of encryption at a time. There should be a minimum communication at a time.

Support for secure group communication: In a communication there are number of processes which coordinate their activities. This coordination must be secure and for this there is no such security policy.

Support for multiple implementations: There should be a security policy which should provide security to multiple sources based on public and private key cryptography.[8]

3. GRID SECURITY CHALLENGES

Multiple resources provide the control policies to the third party. The VO is one which coordinates the resource sharing and use.
The dynamic policies and entry of new participants in the system gives the need for three key functions which are:

Multiple security mechanisms:
Organizations which participate in a VO have investment in security mechanism and infrastructure. Grid security interoperates with these mechanisms.

Dynamic creation of services:
Users must be able to create new services (e.g., “resources”) dynamically without administrator permission. These services should coordinate and interact with other services. So, we must be able to name the service with acceptable identity and should be able to grant rights to that identity without any contradiction with the governing local policy.

Dynamic establishment of trust domains:
VO needs to establish coordination between its user and all the resources so that they can communicate easily. These domains must establish trust dynamically whenever a new user join or leave a VO. A user-driven security model is needed to create new entries of the user so that they can coordinate with the resources within the VO.[4]

4. GLOBUS TOOLKIT SECURITY MODELS

The Globus Toolkit's Authentication and Authorization components provide the basis standard for the "core" security software in Grid systems and applications. Globus software development kits provide programming libraries, Java classes, and essential tools for a PKI, certificate-based authentication system with single sign-on and delegation features, in either Web Services or non-Web Services frameworks. Grid security technology such as GSI and CAS are used to provide security. These technologies are used to represent the security and are used in various grid projects. Web security services work under the OGSA architecture. It is used to represent refactoring, refinement and repacking of various Grid protocols so that better use of useful resources can be done [3].

OSGA is used with the Globus toolkit to provide WSDL for interface to provide Grid services. OSGA is also used to provide an interface for discovery of grid services. Recent goal of OSGA

security work is to provide relationships between OSGA security mechanism and emerging WS security mechanism [9].

4.1 GT2 Grid Security Model

The security technologies incorporated in the Globus Toolkit version 2 (GT2) includes services for Grid Resource Allocation and Management (GRAM), Monitoring and Discovery (MDS), and data movement (GridFTP). These services use Grid Security Infrastructure (GSI) to provide security. GSI works on a common format based on X.509 identity certificates and a common protocol based on transport layer security (TLS, SSL). An X.509 certificate is associated with private key that forms a unique authentication set that a Grid uses to authenticate itself to other Grid entities. [10]

The TLS-based protocol is used to provide message protection (encryption, integrity checking), according to the requirement of data stream. Gateways are used to translate information between common GSI infrastructure and local site mechanisms. For example, the Kerberos Certificate Authority (KCA) provides an interface for translation of Kerberos to GSI and vice versa. [8]

Each GSI certificate is issued by certificate authority (CA), which runs a large number of organization or commercial company. To trust the X.509 communication, the CA issues the certificate to trust the entity. An X.509 identity certificate is used within GSI for establishment of a trusted communication. [11]

In mechanisms such as Kerberos, where for inter-institutional a bilateral agreement is required at the organizational level, trust in a CA is established unilaterally: A single entity can decide to trust any CA, without involving the whole organization. This feature is used in the establishment of VOs in which some portions of the organizations are only used and not the whole organization. [12]

GSI introduces X.509 proxy certificates, which is an extension to GSI used by X.509 identity certificates to allow a user to assign a new X.509 identity to an entity and then delegate subset of their rights to that identity. Users create this proxy certificate by issuing a new X.509 certificate signed by it without involving the CA. By this mechanism new authentication and identities can be created quickly as there is no involvement of the administrator. To create a trusted communication VOs is provided for both the proxy certificate and for security services, Example, the Community Authorization Service (CAS). According to GSI policy if any two entities have proxy certificates issued by the same user they can trust each other. This policy allows the users to create trusted communication itself by issuing proxy certificates to any services with whom they wish to collaborate. [13]

This policy of trust between proxy holders allows then for a easy and simple trust domains but for complicated trust domains they have some limitations, for example, limited trust between multiple parties in which we can use security services such as CAS that allow flexible, expressive policy to be created for multiple users in a VO. CAS allows a VO to use the policy that has been provided to it by the resource providers in the VO. This process has three steps shown in Figure 1:

The three steps of the figure are:

Firstly, the user authenticates to CAS and receives notification from CAS stating VO's policy that how the user may use VO resources.

Second, after that the user presents the details to a VO resource and the usage request.

Finally, then evaluation is done whether to allow the request, for this the resource checks both local policy and the VO policy expressed in the CAS assertion. CAS allows a resource to retain the authority over that resource, but it also allows the VO to control the enforced policy. Then, the VO coordinate the policy that how the resources will be shared.

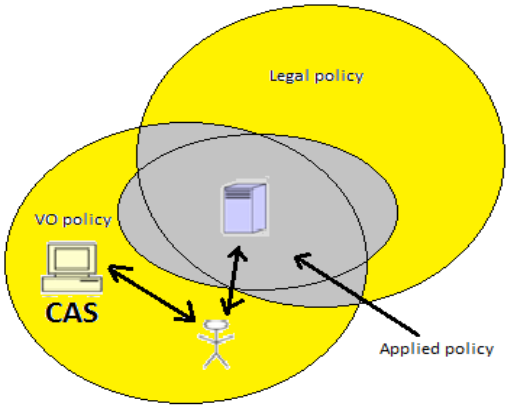

Figure 1. Policy of CAS and VO.

While designing GSI we have several efforts to build on PKI. Some of these efforts with respect to Grid security requirements are:

First, Kerberos needs the site administrators for establishment of inter domain trust between new entities.

Second, the CRISIS i.e. a wide area security system provides a uniform and scalable security infrastructure in a wide area network but does not provide interoperability with local security mechanisms.

Third, Secure Shell (SSH) gives us a system of authentication and message protection but does not support translation between different mechanisms or creation of dynamic entities [14].

4.2 GT3 Security Model

Grid security challenges are solved with Open Grid Services Architecture (OGSA) along with a set of technical specifications to integrate Grid technologies with Web services technologies. Web services technologies allow defining software component in terms of access methods, to bind these methods with specific communication mechanisms, and also to provide mechanisms for discovering relevant services.

There are no particular mechanisms but few are emerging as ubiquitous. The Simple Object Access Protocol (SOAP) provides an interface for messaging using XML along with HTTP. The Web Services Description Language (WSDL) provides a method for expressing operation signatures and also bindings to protocols and endpoints in an XML document.

OGSA is a standard Web service interfaces and behaviors to add Web services with the concepts of crateful services and secure invocation, and also capabilities to address Grid-specific

requirements. These interfaces and behaviors define a “Grid service” and allow users to manage the Grid service’s life-cycle, according to the policies, and create sophisticated distributed services. [6]

A grid service is defined as an interface for service data elements (SDEs) that other entities can query or subscribe to. OGSA introduces new opportunities and challenges for Grid security. Globus Toolkit (GT3) and Grid Security Infrastructure (GSI3) were the first to implement OGSA mechanisms. GT3’s security model allows applications and users to operate on the Grid as easy and automatic manner as possible. Security mechanisms should not be instantiated in an application but should be supplied by the surrounding Grid infrastructure to adapt on behalf of the application to meet the application's requirements. [7]

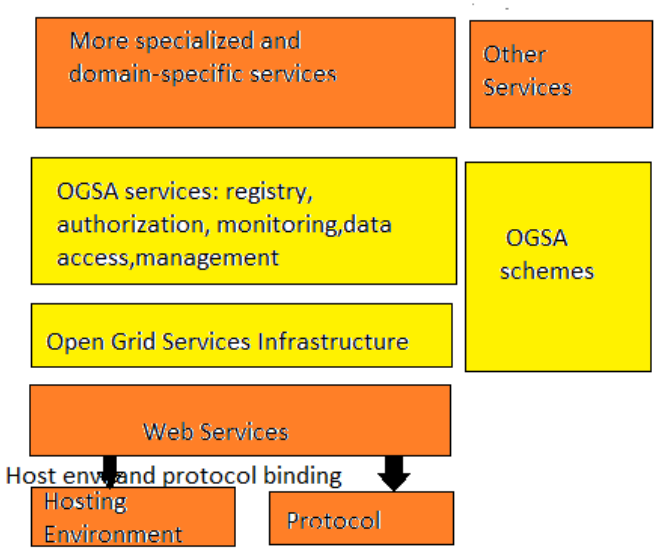

Figure 2. OGSA Architecture

The application should deal only with application specific policy. GT3 uses the following features of OGSA and Web services security to achieve their goals, these goals are to:
First, use of security functionality as OGSA services to locate them and use the service whenever needed.

Second, use of sophisticated host environment to provide security for applications and to adapt security of application without changing it.

Third, to publish service security policy for clients to discover dynamically what are the requirements and mechanisms needed for establishing trust with the service.
Fourth, to provide specifies standards for the exchange of security tokens for interoperability.[4]

4.3 GT4 Security Models

GT4 Authorization implements SAML (security assertion markup language), and uses the XACML (extensible access control markup language). XACML authorization framework architecture is an implementation of the Open Grid Services Architecture is an initiative for recasting Grid concepts within a service oriented framework based on Web services. [14]
In GT4, we have additional Web Services security specifications implementation. Web Services has provided several security standards that which influences Grid computing. XACML and

SAML are the two important authorization standards. We have several other authorization systems that support Grid computing that are Akenti, PERMIS, Shibboleth and VOMS. Akenti, PERMIS and Shibboleth use the type of attributes which are needed to make authorization decision. VOMS provides user attributes used for authorization. These authorization systems have their own policies, and can be integrated with GT4 authorization framework to provide authorization services. [5]

The XACML authorization model has the following policies that are used to create communication. The functioning of these policies are:

Firstly, The PEP (Policy Enforcement Point) is used to accept the access requests from users and then it sends the requests to the PDP.

Then, The PDP(Policy Decision Point) then makes the access decisions according to the security policy or policy set of PAP (Policy Administration Point) and also by using attributes of the subjects, the resource, and the environment that are obtained by querying the PIP (Policy Information Point).

After that, the access decision taken by the PDP is then sent to the PEP. Finally, according to the decision of PDP, the PEP then either permits or denies the access request [9].

The whole architecture is shown below.

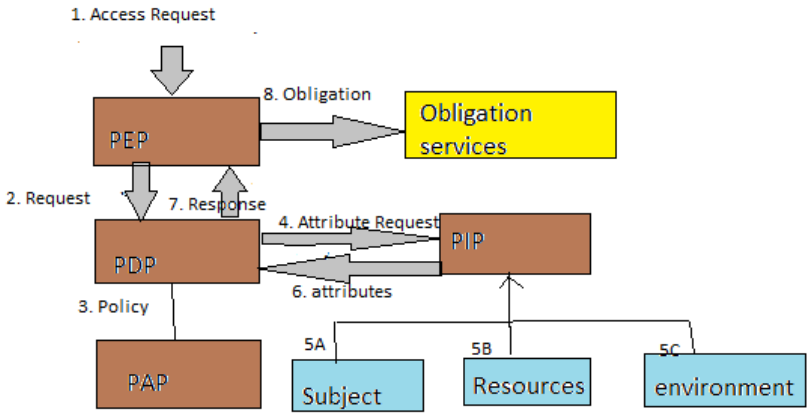

Figure 3. XACML authorization model

XACML also defines a policy language. Policies are organized in hierarchy with the Policy Sets combined using combining algorithms. A rule is has a target, an effect of that rule and a condition on which the rule works. A Policy comprises of a target, one or more rules, and an optional set of obligations [9].

5. SMART GRID CYBER SECURITY:

The cyber security for the smart grid is the possibility that if in a centralized grid we have two way digital communications the grid can become susceptible to the hackers who can use customer confidential information and can cause adverse effect on the communication. This is the latest concern in the Grid to create a Smart Grid cyber security to provide the internet security in the

Grid. There should be some policies with which we can take the benefits of the Internet and also the available computation power in a secure way [1].

Internet facility is much more reliable than electric grid due to the following reasons:
1) Internet is decentralized and is in starfish pattern and not in spider,
2) Asynchronous i.e. we don't have to use a single source we can work on different server and
3) It has many paths and not a few single connections. The Internet is a smart grid, a resilient grid, a self-healing grid that does not go down. The last connection to the grid may fail, or a particular destination may fail.

The Internet makes it possible to have a more secure grid as it reliably monitor and control every part of the grid in real time. The new smart grid will be a less centralized grid because:
1) the traditional economies that supported it has been removed by risk and uncertainty of siting, construction, operation, fuel supply, environmental impact and cost recovery,
2) There is penetration of distributed generation, storage, PHEVs/EVs as well as customer premises energy management systems
3) There is an increasing penetration of stochastic, energy sources like wind, solar and consumer dispatched generation. There is a complex grid with many points to automatically monitor and control resources.

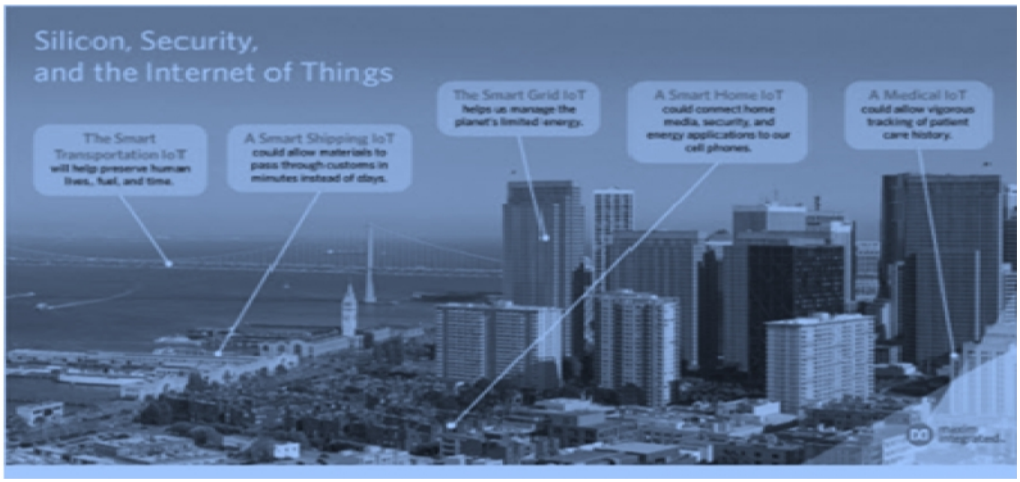

Figure 4- Cyber Grid

5.1 Why cyber security is so hard for the future grid

The following reasons due to which the cyber security will not be implemented so easily in future grid are:

First is, Legacy controllers, networks Fragile security, built to run on private data links, 24/7 (hard to update, patch), real time requirements (security, crypto may impact timing)
Second, Control nets run over (or tunneled though) public networks (attack channel, or subject to broader disruption)
Third, Best Practices for Control Systems & Grid Security (DHS, NERC CIP standards, NIST Draft NISTIR 7628, etc.)
Fourth, these are processes for developing secure systems, not cookbook answers!
Fifth, Security is a system issue—what are the pieces and how do they work together
And the last is- Security is a moving target [2].

Research activity:

- US Government: DHS, INL, NIST, etc.
- Foreign Governments
- Industry Consortia
- Universities, I3P (industry, universities)
- Two Relevant Research Projects at NYU-Poly
- Trusted Platforms: A hardware basis for trusting software, grid element identity, and actions
- INFER—when the defenses have failed.[12]

6. CONCLUSION

Grid computing presents a number of security challenges that are met by the Globus Toolkit's Grid Security Infrastructure (GSI). Version 3 of the Globus Toolkit (GT3) implements the emerging Open Grid Services Architecture; its GSI implementation (GSI3) takes advantage of this evolution to improve on the security model used in earlier versions of the toolkit. Its development provides a basis for a variety of future work. GT4 Security Infrastructure implements the existing and emerging standards which are used by the broader Web Services community. In particular, we are interested in exploiting WS-Routing to improve firewall compatibility; in defining and implementing standard services for authorization, credential conversation, identity mapping; and in using WS-Policy to automate application determination of requirements and location of services that meet those requirements. Also the cyber security in Grid is the latest interest in the field of Grid computing to provide security.

ACKNOWLEDGEMENTS

We would like to thank our principal for providing us the platform for research. Also we are thankful to TEQIP-II for funding this publication. Support of the technical staff was also commendable.

REFERENCES

[1] Report to NIST on Smart Grid Interoperability Standards Roadmap EPRI, Jun. 17, 2009 [Online].Available:http://www.nist.gov/smartgrid/InterimSmartGridRoadmapNISTRestructure.pdf

[2] Draft smart grid cyber security strategy and requirements, NIST IR 7628, Sep. 2009 [Online]. Available: http://csrc.nist.gov/publications/ drafts/nistir-7628/draft-nistir-7628.pdf

[3] "Public key infrastructure," Wikipedia Feb. 18, 2010 [Online]. Available: http://en.wikipedia.org/wiki/Public_key_infrastructure

[4] Energy Assurance Daily, September 27, 2007. U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability, Infrastructure Security and Energy Restoration Division. April 25, 2010.

[5] WiMax Security 2010 [Online]. Available: http://www.topbits. com/wimax-security.html

[6] I. Foster and C. Kesselman, editors. Computational Grids: The Future of High Performance Distributed Computing. Morgan Kaufmann, 1998.

[7] I. Foster, K. Kesselman, The Grid: Blueprint for a Future Computing Infrastructure(Morgan Kaufmann in Computer Architecture and Design), 1999.

[8] Ian, F., C. Kesselman and S. Tuecke(2001). 'The anatomy of the grid: enabling scalable virtual organizations', a reprint in Berman et. al(2003) pp.171-191.

[9] L. Ramakrishnan, Securing Next-Generation Grids, IEEE IT Pro, March/April 2004.

[10] E. Cody, R. Sharman, Raghav H. Rao, Sh. Upadhyaya, Security in grid computing: A review and synthesis, http://www.siencedirect.com (Document view: October 12 2010).

[11] Foster, I., Kesselman, C., Nick, J. and Tuecke, S. The Physiology of the Grid: An Open Grid Services Architecture for Distributed Systems Integration, Globus Project, 2002. http://www.globus.org/research/papers/ogsa.pdf.

[12] Foster, I., Kesselman, C., Tsudik, G. and Tuecke, S. A Security Architecture for Computational Grids. ACM Conference on Computers and Security, 1998, 83-91.
[13] CCITT Recommendation X.509: The Directory – Authentication Framework.1988.
[14] Minoli D. (2005). "A Networking Approach to Grid Computing", Prentice Hall.
[15] Simple Object Access Protocol (SOAP) 1.1, www.w3.org/TR/SOAP

Authors

Mr. Saurabh Maheshwari is an Assistant Professor in Dept. of Computer Engineering in Govt. Women Engineering College Ajmer, Rajasthan, India. He is pursuing Ph.D. in ICT from IIT Jodhpur. He has done his M.Tech. in CSE from MNIT Jaipur, India. His research interests lies in Image Processing, Biometrics, Bio-Instrumentation and Application Development for handheld devices.

Ms. Neha Mishra is pursuing M.Tech in CSE from Govt. Women Engineering College Ajmer India. She has completed her B.Tech in 2012 from RCEW Jaipur India.

Ms. Ritu Yadav is pursuing M.Tech in CSE from Govt. Women Engineering College Ajmer India. She has completed her B.Tech in 2012 from Govt. Women Engineering College Ajmer India.