Security Issues in Grid Computing

Abdur Rakib*

VILL- Pat Pukur, P.O-Digha Patpukur, Distric-Nadia State West Bengal, Pin-741154

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.

----------X----------

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.

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 provide authentication to verify the users, process which have users computation and resources used by the processes to authenticate 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.

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.

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 (Energy Assurance Daily, 2007).)

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.

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 sitting, 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.

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.

Research activity:

- Foreign Governments
- Industry Consortia
- INFER when the defenses have failed (Foster, et. al., 1998).
- Trusted Platforms: A hardware basis for trusting software, grid element identity, and actions
- Two Relevant Research Projects at NYU-Poly
- Universities, I3P (industry, universities)
- US Government: DHS, INL, NIST, etc.

6. CONCLUSION

Grid computing presents a number of security challenges that are met by the Globus Toolkits 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

CCITT Recommendation X.509: The Directory Authentication Framework.1988.

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

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

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.

Foster, I., Kesselman, C., Nick, J. and Tuecke, S. (2002). 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.

Foster, I., Kesselman, C., Tsudik, G. and Tuecke, S. (1998). A Security Architecture for Computational Grids. ACM Conference on Computers and Security, pp. 83-91.

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

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

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

L. Ramakrishnan (2004). Securing Next-Generation Grids, IEEE IT Pro, March/April 2004.

Minoli D. (2005). A Networking Approach to Grid Computing, Prentice Hall.

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

Report to NIST on Smart Grid Interoperability Standards Roadmap EPRI, Jun. 17, 2009 [Online].Available:http://www.nist.gov/smartgr id/InterimSmartGridRoadmapNISTRestructur e.pdf

Simple Object Access Protocol (SOAP) 1.1, www.w3.org/TR/SOAP

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

Corresponding Author

Abdur Rakib*

VILL- Pat Pukur, P.O-Digha Patpukur, Distric-Nadia State West Bengal, Pin-741154

E-Mail – drrakib1978@rediffmail.com