Security and Privacy matters of Grid Computing

Ms. **Tamara Saad Mohamed**

Cihan University

Abstract

This paper is mentioning the privacy policy of Grid Computing used in different concerned sectors of system network. It provides users dynamically shared resources over the internet, but it is also seen that the users usually scared about security threats and loss of control of data and system. Grid computing materializes to be a promising trend for three reasons: (1) its ability to make more cost-effective use of a given amount of computer resources, (2) as a way to solve problems that can't be approached without an enormous amount of computing power, and (3) because it suggests that the resources of many computers can be cooperatively and perhaps synergistically harnessed and managed as a collaboration toward a common objective. In some grid computing systems, the computers may collaborate rather than being directed by one managing computer. One likely area for the use of grid computing will be pervasive computing applications - those in which computers pervade our environment without our necessary awareness.

Introduction

Authentication is performed using digital signature technology (see digital signatures for an explanation of how this works); secure authentication allows resources to lock data to only those who should have access to it.

The **Grid Security Infrastructure** is a specification for secret, tamper-proof, delegatable communication between software in a grid computing environment. Secure, authenticatable communication is enabled usingasymmetric encryption.

Authentication introduces a problem: often a service will have to retrieve data from a resource independent of the user; in order to do this, it must be supplied with the appropriate privileges. GSI allows for the creation of delegated privileges: a new key is created, marked as a delegated and signed by the user; it is then possible for a service to act on behalf of the user to fetch data from the resource.

Overview

World Community Grid assures Members that applications will not damage their systems or invade their privacy in any way. Our agent runs unobtrusively in the computing background and is not invasive. It cannot detect or change any other files or material on Members machines. It can only update project-specific data in its own files.

World Community Grid Members will always be told what projects they are running. They also will have access to Web pages outlining which organizations are providing the project applications and explaining those projects. Members always have the option of opting out of a project which may be the need and orientation of the grid computing.

Members will be able to control how much of their system resources are used by World Community Grid and will be given user preference options on a wide range of factors, including:

1)Whether the program runs as a screensaver or an application
2)When computation and communication can be done
3)Whether connections should be made automatically
4) Which proxies and firewall settings to use

To protect Member privacy, Members are asked to create a member name when they install the World Community Grid Software. This member name is maintained in the Member profile and used to identify each member on the World Community Grid web site and on any scoreboards. .
This is very important and attractive for the grid clients. In our work, we utilize virtualization technology and trusted computing technology to provide a secure and robust virtualization platform. On this platform, we customize the guest virtual machine operating system, strengthen the isolation between virtual machines, and therefore, greatly improve the data privacy of grid services. With our solution, the grid service provider can compromise the availability, but not the confidentiality of the guest virtual machines.

Methodology

We use standard tracking technology on our Web site, commonly known as "cookies," to help us deliver a customized experience to Members. Our Web site will save a small temporary file on your computer only while you are visiting our site; it will be removed when you exit the World Community Grid Web site. Our primary use for cookies is to help us determine which service and support information is appropriate to a Member's machine. Our use of this technology does not mean that we automatically know any information about individual members - we do not involve it or not but it is the protocol. .
In order to run our projects, World Community Grid software automatically detects certain basic information from a Member's machine; this includes info about the Member's processor speed, and set preferences regarding disk space, memory and times to run the projects on the machine. Members will have access to the information about the properties that are measured by the World Community Grid Software and for what purpose this information will be used.

Requirement of Security

Grid systems and applications may require any or all of the standard security functions, including authentication, access control, integrity, privacy, and non repudiation. In this section, we focus primarily on issues of authentication and access control. Specifically, we seek to (1) provide authentication solutions that allow a user, the processes that comprise a user's computation, and the resources used by those processes, to verify each other's identity; and (2) allow local access control mechanisms to be applied without change, whenever possible.

Conclusion

There are security risks in every application downloaded from the Internet, period. However, we take security very seriously at World Community Grid. We have a comprehensive system of technology and policies to protect you, your computer, and the data running on it. The purpose of this review was to provide an extensive literature survey of current research in the area of security in grid computing, and to identify areas of grid computing security in which more extensive research is needed. More importantly, this paper contributes to the overall body of research concerning security in grid computing through the creation of a comprehensive framework for classification of grid security research. The proposed classification system breaks grid research into four main categories, which are system solutions, behavioral solutions, hybrid solutions, and related technologies. System solutions were further divided into system security for grid resources, which involves securing the storage and CPU power donated to the grid by resource owners; and intrusion detection system solutions, which rely on currently existing IDSs or the creation of new IDS to secure the grid.

Behavioral solutions were subdivided into comprehensive policy-based solutions, which rely on policy over technology to provide security and whose policies cover a wide range of topics, and trust-based solutions, which define and quantify trust as a variable to be used for grid security. The hybrid solutions in Section 5 contain the authentication and authorization solutions for grid computing security, which include both system-based and behavior-based topics. Section 6 described related-technology solutions, which borrow from similar technology areas the security solutions that could be ported to grid computing. In the analysis of grid security literature, no one solution is perfect for every grid. Analysis of the individual situation is needed to find that situation's ideal solution.

The measures that we use include, but are not limited to, virus scanning all of our build environments, digitally signing information sent to the World Community Grid Agent, encryption both of locally stored files and files sent to the World Community Grid Agent, and biometric access control to the World Community Grid servers. We do everything we can to keep both the World Community Grid Agent and our server systems as secure as possible. This paper was designed to provide a high level overview of some of the technologies and decisions that need to be made when using these technologies. It includes some practical advice that may help provide direction as you learn more about these technologies. As these technologies become more established and better understood the tools will evolve and will make implementing grids and clusters easier. These technologies may still be in their infancy but the foundation and standards for building better tools that use them have mainly been established and I expect that the use of these technologies will increase significantly in the next few years as the migration from stand alone systems to service oriented and result oriented applications continues to evolve which is the motto of technology and computer world.

References

Aieer: Grid Computing Volume 4

Aieer: Grid Computing Volume 4-i

Aieer: Grid Computing Volume 5-iii

www.fincad.com/derivatives-resources/articles/grid-computing.aspx

http://5thsastech.khi.ac.ir/uploads/COM-O-47_567389531.pdf

I. Foster and C. Kesselman, editors. Computational Grids: The Future of High

Performance Distributed Computing. Morgan Kaufmann, 1998.

Aieer: Grid Computing Volume 2

Aieer: Grid Computing Volume 3

I. Foster, K. Kesselman, The Grid: Blueprint for a Future Computing Infrastructure

(Morgan Kaufmann in Computer Architecture and Design), 1999.

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

P. Shread, Survey finds grid becoming strategic IT investment,

****