IDS based Security approach in Grid computing Environment

Prof. Dashrath Mane

Department of MCA

V.E.S. Institute of Technology, Mumbai, Maharashtra.

E-Mail id: dashumane@gmail.com

Abstract :

Grid is a kind of Distributed Computing Environment, which allows large scale resource sharing and system integration. Grid Computing is a kind of important information technology which enables resource sharing globally to solve the large scale problem. The services and resources in Grid are heterogeneous and dynamic, and they also belong to different domains.

The wide varieties of IDS (Intrusion Detection System) are available which are designed to handle the specific types of attacks. The technique will protect future attacks in Service Grid Computing Environment at the Grid Infrastructure. So the approach mentioned in paper , IDSGCE (Intrusion Detection System – Grid Computing Environment) can provide the fuller protection against the threats in the Grid Environment.

Keywords: *Grid computing, intrusion detection, Grid topology*

1. Introduction

It is very important that the security mechanisms of a system are designed so as to prevent unauthorized access to system resources and data. However, completely preventing breaches of security appear, at present, unrealistic. We can, however, try to detect these intrusion attempts so that action may be taken to repair the damage later. This field of research is called **Intrusion Detection.**

Intrusion detection system (**IDS**) is a device or software application that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts.

In addition, organizations use IDPSes for other purposes, such as identifying problems with security policies, documenting existing threats, and deterring individuals from violating security policies. IDPSes have become a necessary addition to the security infrastructure of nearly every organization.

IDPSes typically record information related to observed events, notify security administrators of important observed events, and produce reports. Many IDPSes can also respond to a detected threat by attempting to prevent it from succeeding.They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment (e.g., reconfiguring a firewall), or changing the attack's content.

2. IDS REQUIREMENTS

2.1 Functional Requirements

Common functional requirements of an IDS being deployed in current or near-term operational computing environments include the following:

- The IDS must continuously monitor and report intrusions.
- The IDS must supply enough information to repair the system, determine the extent of damage, and establish responsibility for the intrusion.
- The IDS should be modular and configurable as each host and network segment will require their own tests and these tests will need to be continuously upgraded and eventually replaced with new tests.

2.2 Performance Requirements

The IDS performance requirements include:

- To the extent possible, anomalous events or breaches in security should be detected in real-time and reported immediately to minimize the damage to the network and the loss or corruption of confidential information.
- The IDS must not place undue burden or interfere with the normal operations for which the systems were bought and deployed to begin with. This requirement makes it necessary for the agents to be cognizant of the consumption of network resources for which they are competing.
- The IDS must be scalable. As new computing devices are added to the network, the IDS must be able to handle the additional computational and communication load.

We can divide the techniques of intrusion detection into two main types.

2.3. Anomaly Detection :

Anomaly detection techniques assume that all intrusive activities are necessarily anomalous. This means that if we could establish a "normal activity profile" for a system, we could, in theory, flag all system states varying from the established profile by statistically significant amounts as intrusion attempts. However, if we consider that the set of intrusive activities only intersects the set of anomalous activities instead of being exactly the same, we find a couple of interesting possibilities: (1) Anomalous activities that are not intrusive are flagged as intrusive. (2) Intrusive activities that are not anomalous result in false negatives. a block diagram of a typical anomaly detection system is shown in Figure below.

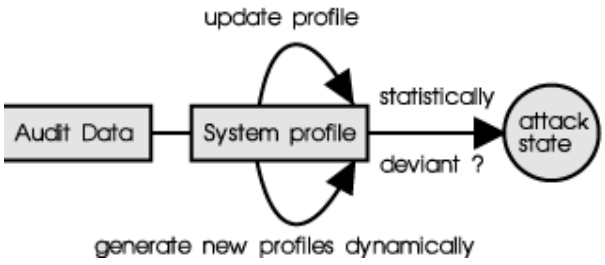


Fig. Anomaly detection

2.4 . Misuse Detection:

The concept behind misuse detection schemes is that there are ways to represent attacks in the form of a pattern or a signature so that even variations of the same attack can be detected. This means that these systems are not unlike virus detection systems they can detect many or all *known* attack patterns, but they are of little use for as yet

unknown attack methods. The main issues in misuse detection systems are how to write a signature that encompasses *all* possible variations of the pertinent attack, and how to write signatures that do not also match non-intrusive activity. A block diagram of a typical misuse detection system is shown in Figure below.

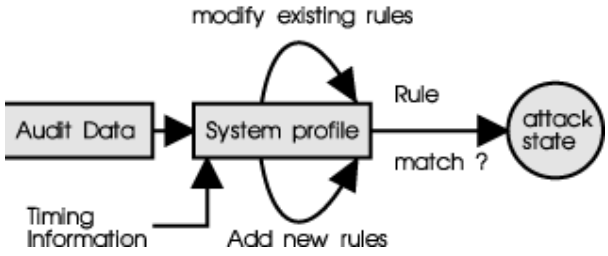


Fig. Misuse Detection

3. Overview of Grid fundamentals

Grid computing combines computers from multiple administrative domains to reach a common goal, to solve a single task, and may then disappear just as quickly.

3.1 Benefits of Grid Computing

To meet set of business requirements you deploy a grid. To better match grid computing capabilities to those requirements, it is useful to keep in mind some common motivations for using grid computing[3].

a. Exploiting under utilized resources

One of the basic uses of grid computing is to run an existing application on a different machine. The machine on which the application is normally run might be unusually busy due to a peak in activity. The job in question could be run on an idle machine elsewhere on the grid.

b. Parallel CPU capacity

The potential for massive parallel CPU capacity is one of the most common visions and attractive features of a grid. In addition to pure scientific needs, such computing power is driving a new evolution in industries such as the bio-medical field, financial modeling, oil exploration, motion picture animation, and many others.

c. Virtual resources and virtual organizations for collaboration

Another capability enabled by grid computing is to provide an environment for collaboration among a wider audience. In the past, distributed computing promised this collaboration and achieved it to some extent. Grid computing can take these capabilities to an even wider audience, while offering important standards that enable very heterogeneous systems to work together to form the image of a large virtual computing system offering a variety of resources, the grid can be organized dynamically into a number of virtual organizations, each with different policy requirements. These virtual organizations can share their resources collectively as a larger grid.

d. Access to additional resources

In addition to CPU and storage resources, a grid can provide access to other resources as well. The additional resources can be provided in additional numbers and/or capacity. For example, if a user needs to increase their total bandwidth to the Internet to implement a data mining search engine, the work can be split

among grid machines that have independent connections to the Internet. In this way, total searching capability is multiplied, since each machine has a separate connection to the Internet.

e. Resource balancing

For applications that are grid-enabled, the grid can offer a resource balancing effect by scheduling grid jobs on machines with low utilization.

f. Management

The grid offers management of priorities among different projects. In the past, each project may have been responsible for its own IT resources and the associated expenses.

Various tools may be able to identify important trends throughout the grid, informing management of those that require attention.

4. Basics of topologies

Grids can be built in all sizes, ranging from just a few machines in a department to groups of machines organized as a hierarchy spanning the world. In this section, we describe some examples in this range of grid system topologies.

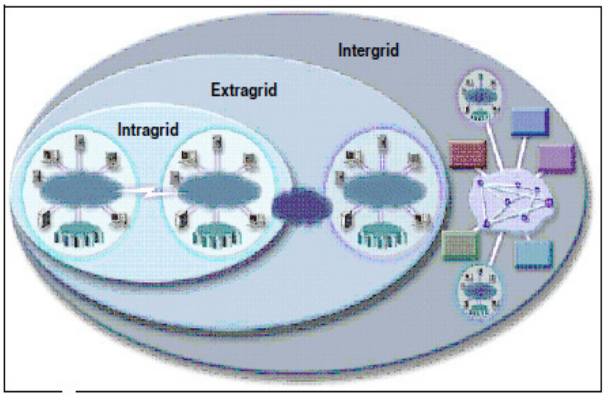


Fig. basic topologies

As presented in Figure simplest grid consists of just a few machines, all of the same hardware architecture and same operating system, connected on a local network. This kind of grid uses homogeneous systems so there are fewer considerations and may be used for specialized applications. The machines are usually in one department of an organization, and their use as a grid may not require any special policies or security concerns.

Machines participating in the grid may include systems from multiple departments but within the same organization. Such a grid is also referred to as an *intragrid*.

Over time, as illustrated in Figure a grid may grow to cross organization boundaries, and may be used to collaborate on projects of common interest. This is known as an intergrid. The highest levels of security are usually required in this configuration. The intragrid offers the prospect for trading or brokering resources over a much wider audience. Resources may be purchased as a utility from trusted supplier

5. Grid services vs. Web services:

Although Grid services are implemented using Web-services technology, there is a fundamental difference between a Grid service and a Web-service.

A Web-service addresses the issue of discovery and invocation of persistent services. A Web Services Description Language (WSDL) compliant document points to a location that hosts the Web service.

A Grid service addresses the issue of a virtual resource and its state management. A grid is a dynamic environment. Hence, a Grid service can be transient rather than persistent. A Grid service can be dynamically created and destroyed, unlike a Web service, which is often presumed available if its corresponding WSDL file is accessible to its client.

6. Grid security Using Intrusion Detection System approach

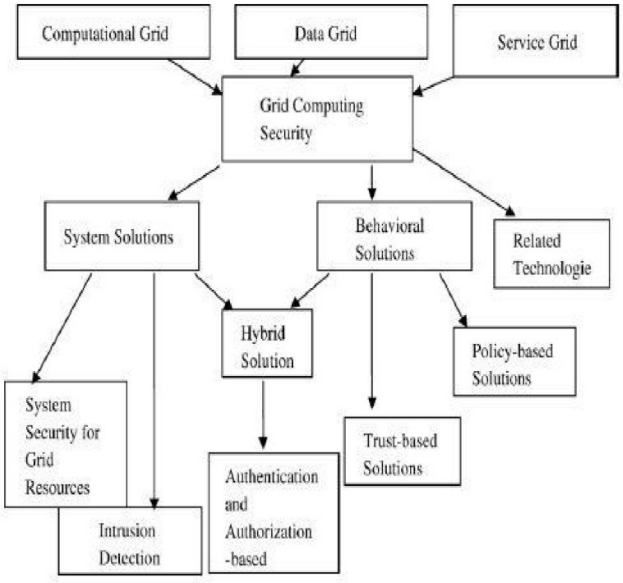
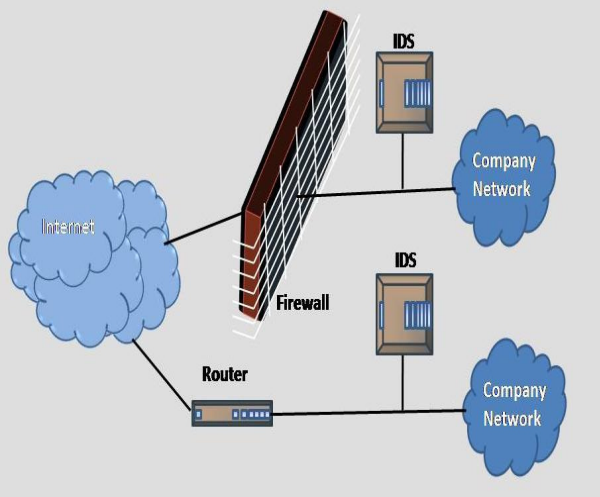


Fig: Grid Security Framework

Grid resources can be quite attractive due to large ranges of computation and storage capabilities and we should expect they become targets for attractors and useful for intruders. The access and sharing of resources and collaborative computing facilitated by Grids amplifies the concerns about intrusions, especially in large scale Grids [2]. In this kind of Grids, the considerable computing power can be used by an Intruder to break passwords, the storage devices can be used to save illicit files, and the large bandwidth networks are ideal for launching Denial of Service Attacks . It is unrealistic to absolutely prevent breaches of security from appearing, especially in complex distributed systems like Grids.

Intrusion detection systems (IDS) in grid computing :

Intrusion detection system (IDS) model for securing the grid environment. an ―intruder into the grid is defined as any grid user who intends to harm the grid or its resources, or intends to use the grid for purposes other than what it was designed for. Rather than being a specific software package , intrusion detection is a technological concept which can be implemented using any one of several software and/or hardware methods.



7. Conclusions

The application of the Grid in real problems will help in building a knowledge base of attack signatures that will enable the use of misuse intrusion detection with the Grid.

An overview of different approaches to ingredient tasks and issues in building an Intrusion Detection System was presented. The findings made will be used to develop an Intrusion Detection System aimed at Grid Computing Environment.

8. References

[1] Kleber Vieira, Alexandre Schulter, Carlos Becker Westphall, and Carla Merkle Westphall **Intrusion Detection for Grid and Cloud Computing 2010 IEEE**

[2] Sanjeev Rana1, Rajneesh Gujral2, Manpreet Singh3 **Securing Grid Using Intrusion Detection System 2009 IEEE**

[3]Bart Jacob Michael Brown Kentaro Fukui Nihar Trivedi ibm.com/redbooks **Introduction to Grid Computing**

[4] Matthew Smith, Fabian Schwarzer, Marian Harbach 2009 11th IEEE International Conference on High Performance Computing and Communications **A Streaming Intrusion Detection for grid computing environments.**

[5] Zohre Zare,Sakine Maleki , 5th SASTech 2011, Khavaran Higher-education Institute, Mashhad, Iran. May 12-14. **Security in grid computing**

[6] Sundaram A., "An Introduction to Intrusion Detection".