International Journal of Recent Trends in Engineering & Research
ISSN(ONLINE) : 2455-1457
IMPACT FACTOR : 3.344

An Advanced Analysis on Grid Computing Security Threats

Amarbir Singh[1], Sarabjit Singh[2]
[1]Department of Computer Science, Guru Nanak Dev University, Amritsar (Punjab)
[2]Department of Computer Science, Guru Nanak Dev University College Verka, Amritsar (Punjab)

Abstract— Grid computing is a distributed computing and storage infrastructure which provides high end computing or supercomputing capability by sharing the resources of computers over the network. To achieve grid computing, development of secure and friendly environment is required. Even being a trustworthy computing environment there are number of threats a grid has to face. A grid can face security hazards due to defenselessness, security compromises, getting hit directly by hackers, security breaches and many more. This paper analyzes the complete analysis of various threats to grid and the possible solutions of it.

Keywords—Grid Computing; Data Grid; Snooping; Brute Force Attack; Grid Architecture

I. INTRODUCTION

Today is the era of computers and we are living in network world. The computing capability of computers is too high these days, so a large amount of computing power goes unused and lot of resources are under utilized in a computing system which may be a computer system spread over wide area, a server or a single PC. On an average each day systems work at their peak approximately for just about 5% of time and for remaining 95% of time they remain idle, which is like a company having schedule to run 24 hours and 7 days a week remain open but no production happen for 5 to 6 days a week. To overcome this situation and implement computer resources efficiently Grid technology is developed [1].

Grid computing makes a virtual high performance computer system by uniting number of computers working together in a single pool, and by using the resources of these systems as an enterprise can obtain the enough computing power for its specific purpose. Grid provides the large computational power of parallel processing by coordinating dependable and consistent computational capabilities at lower expense [2]. The most important underlying technology to make a grid is computer networks. Also it is difficult, limited and expensive for an organization to maintain its own distributed system due to various limitations such as processing, network bandwidth and storage capacity. Having these capabilities for an organization requires continuous modifications and additions which can be pretty much expensive. A step ahead to internet which provides the capability to share files, project modules, grid computing provides the advantage of using and sharing the computational power, storage and other resources of computer systems over a network each in its own administration control. Same process can run on different operating systems and different hardware architectures. So grid computing provides a way to transform a difficult to manage computer into a large virtual computer which can be managed with ease [3].

II. GRID CATEGORIES

Grid is broadly divided [1] into two categories

2.1 Computational Grid

Its focus is on intensive computing problem that is collection of distributed computing resources, aggregated to act as a unified processing resource or virtual supercomputer [4]. Collecting these resources into a unified pool involves coordinated usage policies, job scheduling and queuing characteristics, grid-wide security, and user authentication. The benefit is faster, more efficient processing of computation-intensive jobs, while utilizing existing resources.

2.2 Data Grid

Its focus is on managing enormous (can be said unlimited data) fragmented and distributed data of wide area, secure access to current data. Data grids enable users and applications to manage and efficiently use database information from distributed domains [5]. Much like computational grids, data grids also rely on software for secure access and usage policies. Data grids can be deployed within one administrative domain or across multiple domains. Data grids eliminate the need to unnecessarily move, replicate, or centralize data, translating into cost savings.

III. THE GRID ARCHITECTURE

The architecture [6] of a grid is often represented in layers according to respective functioning. The Architecture which specifies the building of a grid is as follows.

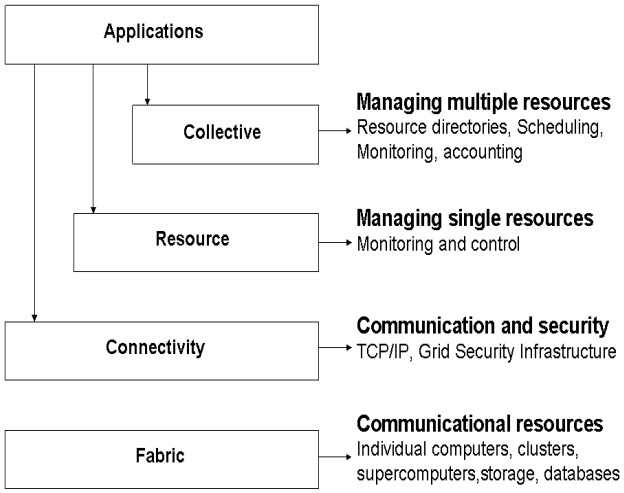

Figure 1. Grid Architecture

IV. SECURITY ISSUES AND ITS REMEDIES

There are large numbers of building blocks which make grid and should be taken under consideration these are hardware, software, users, job scheduling and security for making grid work efficiently. As Grid is a shared environment, and sharing also introduces security problems. As far now, security has been focused on two-party client-server interactions, but Grid involves many more entities, such as precise performance, and involves more complex activities such as collective operations and the downloading of code [7].

Unlike Internet where authentication works efficiently for user accountability, because users are limited to access the domains according to protocols and communication. But a grid is a different case because it provides to the user more power. So we shall discuss some security threats which can be happen to a grid. Some of these threats that can be faced by Grid are as follows.

4.1 Random Users

The Grid is cohesive group of shared resources [10] under their respective administrative domains over Internet. A task submitted by user at one domain of grid can be processed over different domains (resources), for such domains other than that particular domain on which user submitted job, user remains unknown. Being unknown if the user submits malevolent code, he can bring damage either by getting special privilege or can retrieve information from grid domains. An unknown user can join the system and break in system's access control, by doing so such user can attain access to records, programs of an enterprise. A user can control the system activities by getting special privilege and can restrict or stop the system to its job.

The solution for this problem is obviously contain authentication and authorization of the users, these are the conventional mechanisms till used in single domain network based computing areas like Internet for providing one's identity and proper privileges to perform the operation for which he wished-for. These methods are also introduced in case of grid computing but here scenario is different. As we have discussed in threat that a user (say u1) can be trustworthy to one grid (say G1) of an organization [8]. The grid G1 can be part of virtual organization (VO) made up by shared resources of other grids, for some grids which are also part of the virtual organization grid G1 can be unknown. In this case possibility exists that the task submitted by that user U1 processed at resources of unknown grids. In this case question arises that how authorization of U1 to G1 works to unknown grids? The solution to this problem requires a special procedure for authentication of user. This can be achieved by developing trust between the grids even if these are unknown to each other, so the Grids needs to be extremely flexible, and have a reliable accounting mechanism. If we refer to the figure of Grid Architecture the security issue lies in connectivity layer which has responsibility of scheduling and monitoring the activities of network traffic for that it uses middleware, the software that organizes and integrates the computational facilities belonging to a Grid. Its main role is to automate all the "machine to machine" (M2M) negotiations. So the solution to make trust between grids can be the achieved by introducing special algorithms to middleware so they provide global authentication, that means that a user authenticated to one grid get automatically authenticated to unknown grids due to trust generated by middleware.

4.2 Counterfeit (Non Genuine) Grid

Grids in their early days existed were maintained by their respective organizations that were dedicated to research purposes. Now grids are getting commercial and so are getting adopted by enterprises very rapidly by taking under consideration of business profits. Open source makes the task easier. An organization can make a strategy to fulfill its profitable task by making the people provide their home computer system's resources by showing that it is running grid for some charity purpose by giving some avarice on the basis of point or maximum time of providing resources, but false grid always be a big threat for global. This problem can solve by allowing only trustworthy grid or to use firewalls to protect intrusion.

4.3 Snooping

In such threats individual can be interested in the information exchange between grid domains. Such information transfer can be tapped or watched without upsetting the resources. Snooping can be brings into play to spy the serious information, and can be used to implement other types of attacks that can be reply attack, obtain unauthorized privilege, affects the traffic of the network etc [9]. It can be serious case for grid having put into services by government or defense organization of the country.

Cryptography technique PKI (Public Key Infrastructure) and firewall can prevent the grid to get target of snooping. That provides for trusted third party inspection, and guarantee for, user identities. It also allows binding of public keys to users. Firewalls can be used to stop the unwanted traffic on network to get in the grid network.

4.4 Pretense (False show of intentions or motives)

During a communication when one legitimate grid entity is fooled by another suspicious grid entity which is pretending as a valid entity. This type of security attacks may result in the disclosure of confidential information etc. for example, if two grids are running by two organizations say org1 and org2, sharing common data from the same resource R32 of grid running by organization org3 at same time, org1 grid may be interested to check what transaction is going on by org2, org1 can undertake some illegal acts to obtain the information in which that may be interested.

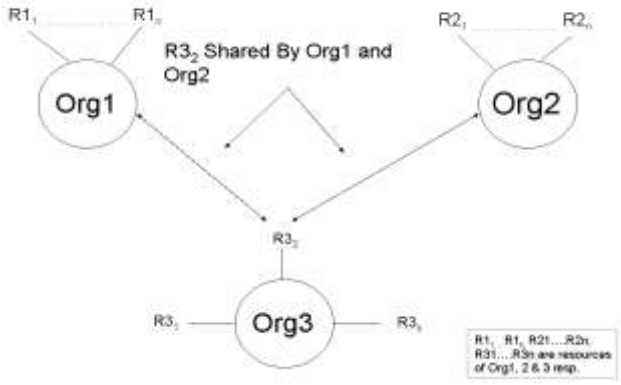

Figure 2 Pretense

This problem can be overcome first by data confidentiality and separate space allocation to separate grid entities at same resource. Sensitive information must not be shown to parties that are not meant for. The confidentiality can be obtained by data encryption of each entity and the separate space allocation can be done by hiding information of one grid's entity form other grid's entity on the resource.

4.5 Distributed Denial of Service (DDOS)

It depicts the security breach which prevents the normal use of some communication facilities. It is getting a common threat to business over the internet as grid system based on Internet so it can be a common target of DDOS attack. Over 2,000 distinct such attacks have recorded per week. It is designed to bring the network down by flooding it with useless traffic. DDOS attacks take advantage of limitations in the TCP/IP protocols. A user begins a DDOS attack by exploiting vulnerability in one system and making it the DDOS "master." It is from the master system that the intruder identifies and communicates with other systems that can be compromised. The intruder loads cracking tools on multiple sometimes thousands of compromised systems. With a single command, the intruder instructs the controlled machines to launch one of many flood attacks against a specified target. The flood of packets to the target causes a denial of service.

Prevention of DDOS relies in knowledge of enemy's tactics and methods. Security policies and procedures should be developed to ensure that best practices are followed. Security policies are a very important part of grid's overall security architecture. Acceptable Use Policy (AUP) is a key tool for removing abusive users from grid network. A response team can be established that is responsible for responding to attacks.

4.6 Brute force attacks

It is a method of defeating a cryptographic scheme by trying a large number of possibilities; for example, exhaustively working through all possible keys (user name, password) in order to decrypt a message. It describes a security threat within the enterprise domain where the attacker can try to decipher the encrypted corporate data, by working through every possible key on the piece of cipher text, until a translation into plaintext is obtained, and if he gets successful he can login easily into a system.

As we have referred PKI solution that does not mean that grid system is completely secure. There are still vulnerabilities exist for which we have to be aware. It is necessary to always keep an open mind and understand that with any networked environment there is going to be some risk involved. Within a PKI environment, we always have to worry about the locations of private keys of grid entity and thefts of digital certificates.

IV. CONCLUSION

In this paper we have analyzed all the aspects of security threats that are possible on the grid. The study shows that there is remedy for all of these threats. It is also found that as new solutions to threats are being found or modified newer threats are also introduced. So it requires continuous research to deal with new threats. The future of grid is very bright if we use it in proper and secure way.

REFERENCES

1. What is the Grid? A Three Point Checklist, Ian Foster
2. Enabling Applications for Grid Computing with Globus, IBM Redpaper
3. Fundamentals of Grid Computing, IBM Redpaper, Viktors Berstis
4. Managing a grid, Part 1: Network and infrastructure, Martin Brown, http://www-28.ibm.com/developerworks/grid/library/gr-manage1/#N10122
5. Managing a grid, Part 2: Security considerations/Aspects, Arun Chhatpar, http://www-128.ibm.com/developerworks/grid/library/gr-manage2/#N10122
6. Foster, C. Kesselman, and S. Tuecke, "The Anatomy of the Grid: Enabling Scalable Virtual Organizations", International J. Supercomputer Applications, 2001.
7. Foster, C. Kesselman, G. Tsudik, S. Tuecke: Security Architecture for Computational Grids. Proc. 5th ACM Conference on Computer and Communications Security Conference, pg. 83-92, 1998.
8. Randy Butler,Von Welch, DouglasEngert, Ian Foster, Steven Tuecke, John Volmer, Carl Kesselman: A National-Scale Authentication Infrastructure
9. W. Mao, F. Yan and C. Chen. Daonity: Grid Security with Behaviour Conformity from Trusted Computing In 1st ACM Workshop on Scalable Trusted Computing
10. Ali Raza Butt, Sumalatha Adabala, Nirav H. Kapadia, Renoto Figueiredo, José A.B. Fortes: Fine-Grain Access Control for Securing Shared Resources in Computational Grids. Proceedings of the International Parallel and Distributed Processing Symposium (IPDPS.02) 1530-2075/02

