Grid Security: Evaluation of Active and Passive Attacks with Proposed Countermeasures

1Nureni Ayofo Azeew, 2Iyamu Tiko, 1Isabella M. Venter, 3O.F.W. Onifade and 4R.A. Azeew
1Department of Computer Science, University of the Western Cape, Private Bag X17, Bellville, 7535, South Africa
2Department of Informatics, Faculty of Information and Communication, Pretoria South, South Africa
3Department of Computer Science, University of Ibadan, Nigeria
4Department of Computer Science, Fountain University, Osogbo, Nigeria

Corresponding Author: Nureni Ayofo Azeew, Department of Computer Science, University of the Western Cape, Private Bag X17, Bellville, 7535, South Africa

ABSTRACT

Grid computing is an emergent computing innovation which offers endless access to computing infrastructure across various organizations (academia and industry). Since this technology allows aggregation of various computer systems for usage by different users to run applications, the information stored on it which may be sensitive and private, remains vulnerable. According to related research on the attribute based access control for grid computing there is no adequate and appropriate security mechanism to authorize and authenticate users before accessing information on a grid system. The issue of security in grid technology has not been fully addressed even though it is a precondition for optimizing grid usability. In this paper therefore, we try to explore some of the main security attacks on a grid system and provide reasonable countermeasures to handle the situation. Finally, an architectural model to prevent any form of attacks explained is also presented.

Key words: Security, active, passive, attacks, grid, topology, countermeasures

INTRODUCTION

For any grid participant to enjoy the full benefits of resource sharing, distribution and aggregation across various domains assurance has to be given that data to be shared is saved from any form of attacks. In a distributed environment like grid as depicted in Fig. 1 which involves users from various domains there is bound to be data manipulation, alteration and falsification. All these are done to suit the aim of adversary to perpetrate his evil act on the grid.

Fig. 1: A simple grid network
Fig. 2: Grid classification based on topology

Some of the problems that have emanated from this circumstance (security attacks) are so devastating and catastrophic so much so that participants in a distributed environment are entertaining fear of sharing and distribution of resources.

This study therefore, attempts to explain various security lapses (Ayofe and Oluwaseyifunmitan, 2009) in a grid based environment and propose various measures to circumvent some of these anomalies.

GRID CLASSIFICATION BASED ON TOPOLOGY

Grid Computing can be classified base on topology into four main groups. They are Clusters, intra-grids, extra-grids and inter-grid (Foster et al., 2004) (Fig. 2).

Cluster: This is the smallest form of grids both in scope and size (Alfawair et al., 2007). This is a combination of various servers to generate high computing power in comparison to what is obtainable in offline system (standalone). This form of grid computing is developed to solve problems in a unit or same department and it is usually implemented in a campus intranets.

Intra-grid: This is a combination of various clusters. This form of grid computing is also known as campus grids. It allows resources to be shared across various departments and units. Intra-grid allows resources to be shared across various organizations under the same policies without any need to address the security and policy management relating to global grids.

Extra-grid: This is type is also called “Partner grids” and “Extraprise grids”. It is a combination of two or more intra-grid with various security domains. This form of grid is geographically distributed between various establishment, companies and organization. Virtual Private Networks (VPN) are used for implementing this type of grid to make resources easily available (Alfawair et al., 2007) to users.

Inter-grid: This type of grid is the final phase of grid evolution. It is otherwise known as global grids. It is a combination of both the intra-grids and cluster grid joined together by the internet. This form of grid is popularly used in academia.

SECURITY ATTACKS ON A GRID SYSTEM

It has been recognized by researchers that all forms of distributed systems are vulnerable and not completely secured. Some of the security measures are inflexible and not scalable (Laccetti and Schmid, 2007).
Security attacks on a grid system can be divided into the following categories:

- Passive attacks
- Active attacks
- Dictionary attacks

**Passive attacks:** Passive security attacks ranges from (Al-Bayatti et al., 2010) secret monitoring of transmissions, such as electronic mails, file exchange on any distributed system, client-server transmission or eavesdropping.

Passive attacks involve a thorough analysis of traffic as well as exposing and releasing of message content.

- **Release of message contents:** This form of attack can be best explained with Fig. 3. It is obvious that electronic mail message, telephone conversation and a file being transferred may contain sensitive and confidential information (William, 2002).

To guard against the vulnerability of the information, there is need for preventing the opponent form learning and understanding the contents of the transmission (Welch and Lathrop, 2003).

- **Traffic analysis:** This is a form of security attack (Ayofe and Oluwaseyifunmitan, 2009) whereby messages are intercepted and examined in order to get information from patterns in communication process. This form of attack can be carried out even when the message is encrypted and is difficult to be decrypted. Summarily, the higher the number of messages intercepted and examined the more deduction and inference from the traffic. Traffic analysis can be carried out in military intelligence and it is a serious concern in computer security (McClure et al., 2003) (Fig. 4)

Supposing a message is masked (encrypted), an adversary might still try to know and understand the pattern of the message by determining the location and identity of communicating host and probably determine the frequency (William, 2002) as well as the length of messages being transferred. It has been established that passive attacks are complex to detect since they have nothing to do with alteration of the data.

![Fig. 3: Release of message contents (Passive attack) Source: William (2002)](image-url)
Active attacks: This type of attack attempts to change, remove, or destroy data being transferred from one system to another system on a grid network. Some of the types of active attacks are denial of service, masquerade, replay and modification. An active attack can be both internal or external (Welch and Lathrop, 2003). It can be prevented with the aid of common and popular security mechanisms like firewalls and encryption techniques.

The section below gives a brief explanation of some of the examples of active attacks:

- **Denial of service (DoS):** This is a type of active security attack which halts the system on a grid (IASTED, 2004) so that it fails to respond to users’ demand. To accomplish this objective, attackers will send a very large quantity of data at the access point (Hussain, 2005) so that it makes it extremely difficult to respond appropriately. DoS deliberately aims at preventing legitimate grid users to have access to the resources on the grid.

- **Impersonation:** In this case the attitude as well as behaviour of an authorized grid user are mimicked and copied by the attackers. With this approach, attackers can easily modify and change information to the detriment of a legal user. Man-in-the-Middle attack is the commonest form of impersonation.

- **Disclosure:** Sensitive information across the grid might be disclosed by a compromised machine on the grid to another machine that is not authorized to have access to such information. Also, classified information might be divulged by a user that is not recognized to access it thereby exposing the secrecy therein (Al-Bayatti et al., 2010).

- **Unauthorized access:** This type of security attack occurs when a person that is permitted to access particular information gains access to it and play around with it as if he is the rightful owner of the information. When this happens the sensitivity of the information will be lost and manipulation can easily be made without any challenge (IASTED, 2004). This may happen through unpatched software or other vulnerabilities that are known.

- **Replay attack:** Replay attack can also be likened to “Man in the middle” form of attack. This form of security attack allows the data packets to be intercepted and replay (resend) to the server. For example, if a client sends a password and a username that is encrypted to a server to gain access to any grid information and a hacker is able to use a monitoring software to intercept such a message and replay/resend it, such a hacker will have the same rights the rightful owner of such a message (IASTED, 2004). In fact, the hacker may even as attempt as to alter such password and thereby deny the authorised user access to the information. This type of attack can be avoided with the aid of digital signatures.
Dictionary attack: This method is used by attackers to break a security measure put in place for a system or a server, by trying all possible passwords with the intention of gaining access. They (attackers) begin by using the most common way people create a password for example name, places, date of birth and place of work. The attack is carried out with the assistance of software. This form of attack allows words to be sorted by usage frequency and begins with the most likely one.

Dictionary attacks allow spammers (Ayofe et al., 2010a) to randomly send mail across to various addresses using a combination of some popular domain names with the intention of getting information across to a large percentage of e-mail users (Pinka and Sander, 2008). For example a dictionary attack may begin with the following e-mail addresses john@uwc.ac.za, john1@uwc.ac.za, john2@uwc.ac.za, john3@uwc.ac.za. This may continue till all possible combinations of both the numbers and variable has been tried and exhausted.

Account locking and delayed response are two major countermeasures against any form of dictionary attacks. Account locking allows the accounts to be locked completely to the attackers after making a few unsuccessful efforts to gain access. In delayed response, a server gives a slow YES/NO response when a login-name/password is supplied. This prevents shield attackers from consistent and frequent checking various passwords (Pinka and Sander, 2008).

SECURITY REQUIREMENTS IN A GRID ENVIRONMENT

In order to shield (Lu et al., 2008) the resources on the grid from being attacked and also from unlawful visitation, a reliable privacy; data integrity; data confidentiality; non-repudiation; availability; authorization as well as authentication (Hamid et al., 2009) must assured and provided.

Authorization: For any organization to allow its resources to be jointly shared (Ayofe et al., 2010b) between all parties involved there is need for authorization as per who should have access any particular resources and who should not. It also allows that permission is given to only the authorized nodes on the network (Al-Bayatti et al., 2010). Globus Toolkit Gridmap files, The Community Authorisation Service (CAS), Virtual Organisation Membership Service (VOMS are authorization measures usually adopted in grid computing (Chadwick, 2005).

Authentication and access control: Impersonation has been identified as a big threat in a grid environment. Authentication is important to purposely prevent the resources from illegal access (Lu et al., 2008).

The main purpose of authentication (Hoque and Avery, 2010) is solely to confirm that the user is he who claims to represent and not any other person.

As shown in Fig. 5, for a man standing to access resources being deposited by terminals T1 and T2 on a server, there is need for authentication.

In both the shared and personal computer system, authentication is usually carried out with the use of a password and username. It has been established that when a password is used to log into the system, the authenticity of a user is usually fully guaranteed. However a password can be stolen hence the information on the system can be vulnerable.

Digital certificates, verified by a Certificate Authority (Lu et al., 2008), is taken as the best way to ensure authentication on the internet.
**Fig. 5:** Authentication by a server

**Availability:** Irrespective of security attacks, data must be readily available across the network to satisfy the demand of grid computing user at any point in time. Data availability means that data is available at all times. In a grid environment, data availability is usually achieved through redundancy; which has to do with how data is stored and how such data can be reached. Also, essential and adequate services must be made available by a node at any time (Fran *et al.*, 2005).

**Data confidentiality:** The purpose of data confidentiality is to protect data from being divulged to the wrong or an unintended party (Shen *et al.*, 2006).

Two steps can be used to achieve data confidentiality; data encryption and data decryption. Also, two main types of cryptography can be used to provide data confidentiality (MSDN, 2005), they are: symmetric and asymmetric.

**Symmetric cryptography:** In this type of cryptography both the sender and the recipient use a common key to carry out encryption and decryption (Fig. 6).

As illustrated in Fig. 6, symmetric encryption involves the following stages:

- The ciphertext message is created by the sender through the encryption of a plaintext with the assistance of a symmetric encryption algorithm as well as a shared key
- The ciphertext message is sent to the recipient by the sender
- The ciphertext message is decrypted back into a plaintext by the recipient

**Asymmetric cryptography:** With asymmetric cryptography also called public key cryptography; different keys are used by the sender and recipient for encryption and decryption respectively (MSDN, 2005). The sender encrypts data with one key and the recipient uses a different key to decrypt ciphertext (Fig. 7).

As illustrated in Fig. 7, asymmetric encryption involves the following steps:

- The ciphertext message is created by the sender who encrypts the plaintext message with the aid of an encryption algorithm and the recipient’s public key
- The ciphertext message is sent from the sender to the recipient
- The ciphertext message is decrypted back to plaintext with the aid of a private key that tallies with the public key that was used to encrypt the same message
**Data integrity:** In the banking industry, military operation as well as aviation industry data modification by unauthorised (Zanjani et al., 2009) person may result in a serious casualty. With data integrity, guarantee is assured that data in a grid environment is removed, updated, modified, deleted, edited and transmitted only by an authorised (Prasannakumari, 2009) fellow.

**Non repudiation:** Since transactions take place often on the internet, this security service protects the parties involved in a transaction from denying that a particular transaction has taken place when such a transaction has been carried out.

Non-repudiation therefore ensures that both the receiver and the sender cannot renege or deny that a message has been sent or received. This security (Ayofe and Lawal, 2010) measure can assist in knowing, detecting as well as isolating (Onieva et al., 2008) any node on the grid that is compromised.

This security measure is usually achieved through the use of Digital signatures and certificates. Timestamps which contain the date and time can equally be used. Finally, a message transfer agent can be used to create and provide a digital receipt to establish that a message(s) were sent and/or received.

**Privacy:** The main purpose of privacy (Rasheed et al., 2010) is to ensure that information being shared on the grid system is protected. Every grid user wants his sensitive information to be
completely secured from misuse and abuse. According to Alan Westin, the definition of privacy is given as follows: (Kagal and Abelson, 2010):

- "Privacy is the right of individuals to determine for themselves when, how and to what extent information about them is communicated to others"

Proposed secured grid model: As shown in the Fig. 8, when a message is to be sent from location A to location B across a grid software (Trusted Third Party). Both the sender and the receiver are expected to work with cooperation in order to ensure smooth exchange of information across the grid network. A reliable information channel is on ground to ensure smooth passage of message from the source to destination. The security of information is very crucial and vital to protect the message flow from adversary who may tamper with the confidentiality, authenticity and integrity.

How do we ensure a secure transmission? With this model, an encryption key is used with the transformation to protect the message before transmission and unprotect it immediately at the receiving end of location B. This will make the message unreadable by the opponent. Also, there is an addition of a code based on the message contents which can be used to trace and identify the identity of the sender which should remain unknown to the opponents.

CONCLUSION
Since the integrity, confidentiality as well as integrity of information being sent across a distributed system remains sacrosanct, it is therefore crucial to ensure that appropriate mechanism is on ground to ensure that the original nature of information is not tampered with. Having identified various security lapses in a grid-based environment with countermeasures suggested, it our strong believe that implementation of the model and measures offered against theses security challenges with be of great use in securing our information.

REFERENCES

