Network Security: Goals, Services and Mechanisms in Grid Computing Environments

Ajay Kumar
Mewar University, Chittorgarh,
Rajathan India

Dr. Seema Bawa
Thapar University, Patiala,
Punjab, India

ABSTRACT

Grid computing is widely regarded as a technology of immense potential in both industry and academia. The evaluation pattern of grid technologies is very similar to the growth and evolution of Internet technologies that was witnessed in the early 1990s. Similar to the Internet, the initial Grid computing technologies were also developed mostly in the universities and research labs to solve unique research problems and to collaborate between different researchers across the world.

As an issue, security is perhaps the most important and needs close understanding as Grid computing offers unique security challenges. In this research paper we look network security goals and services. Also, we identify the some security mechanisms.

Keywords: Network Security, Grid, Security Services, Authentication, Cryptography, Access Control.

1. INTRODUCTION

Security is the freedom from danger or anxiety and a situation with no risk, with no sense of threat. Some of the basic properties of security are[1][2] - confidentiality, integrity, availability, authentication, nonrepudiation etc. Confidentiality is the properties of protecting the content of information from all users other than those intended by the legal owner of the information. Integrity is the property of protecting information by unauthorized users. Availability is the property of protecting information from unauthorized temporary or permanent with holding of information. Authentication is divided into peer-entity authentication and data origin authentication. Peer entity authentication is the property of ensuring the identity of an entity, which may be a human, a machine or another asset such as a software program. Data origin authentication is the property of ensuring the source of the information. Nonrepudiation is the property of ensuring that principle that have committed to an action cannot deny that commitment at a later time. In a practical approach, IT security involves the protection of information assets. Assets may be – physical (e.g. computer, network infrastructure elements, building hosting equipment), data (electronic files, databases), software (application s/w, configuration files).

The protection of assets can be achieved through the prevention, deletion or recovery of assets from security threats and vulnerabilities. A security threat is any event that may harm an asset. When security threat is realized an IT system or network is under a security attack. The impact of the threat measures the magnitude of the loss that would e caused to the asset or asset owner if the threat were realized against it.

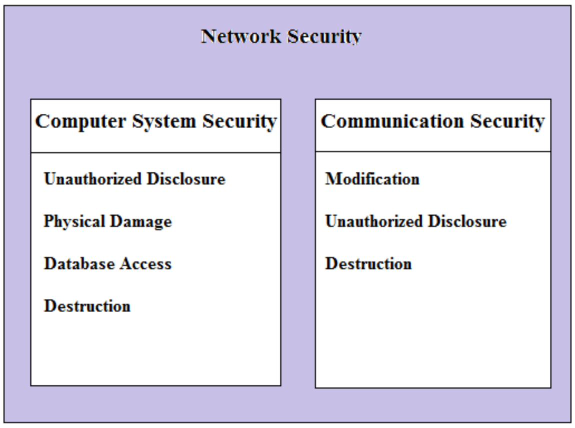

Figure 1: Network Security System

Generally, the communicating entities in a computer network are principles, subjects or entities. The principles can be further divided into user, hosts and processes. A user is a human entity responsible for its actions in a computer network. A host is an addressable entity within a computer network. Each host has a unique address within a computer network. A process is an instance of an executable program. It is used in a client-server model in order to distinguish between the client and the server process. The network security can be considered through the achievement of two security goals:

- Computer system security
- Communication security

The goal of computer security is to protect information assets against unauthorized or malicious use as well as to protect the information stored in computer systems from unauthorized disclosure, modification or destruction. The goal of communication security is to protect information during its transmission through a communication medium from unauthorized[6][7].

2. SECURITY SERVICES

The security objectives are accomplished through security policies and security services[8][9]. A security policy is the set of criteria that define the provision of security services, where a security service is a service which is provided by a layer of communicating open systems, in order to ensure adequate security of the systems or of data transfers. The basic security services are following:

- Authentication
- Access control
- Data confidentiality
- Data Integrity
- Nonrepudiation

Authentication service may be used to prove that the claimed identity of a communicating principle is valid (peer entity authentication) or that the claimed source of a data unit is valid (data origin authentication). **Access control** service can be used to protect the information assets and resources available via OSI from unauthorized access. It also applied to various types of access, such as read, write or execute or combinations of the above. **Data confidentiality** service protects the data from disclosure to unauthorized principles. It includes: connection confidentiality, connectionless confidentiality, selective field confidentiality, traffic flow confidentiality. **Data Integrity** service ensures that during their transmission the data is not altered by unauthorized principles. **Nonrepudiation** services that a principal cannot deny the receipt of a message. This may take one or both of two forms. (1) with nonrepudiation with proof of origin recipient of data is provided with proof the origin of data, so that the sender later deny that he or she sent the particular data. (2) with nonrepudiation with proof of delivery the sender of data is provided with proof of the delivery of data, so the receiver cannot later deny having received the particular data.

3. SECURITY MECHANISMS

The implementation of the security services is provided through security mechanisms. These mechanisms are:-

- Encipherment mechanisms
- Digital Signatures
- Access Control mechanisms
- Traffic-padding mechanisms
- Routing Control mechanisms
- Notarization mechanisms

Encipherment mechanisms provide data confidentiality services by transforming the data forms not readable by unauthorized principles. It can also component a number of other security mechanisms. These mechanisms concern with two keys: public key and private key. Here the knowledge of public key does not imply knowledge of private key.

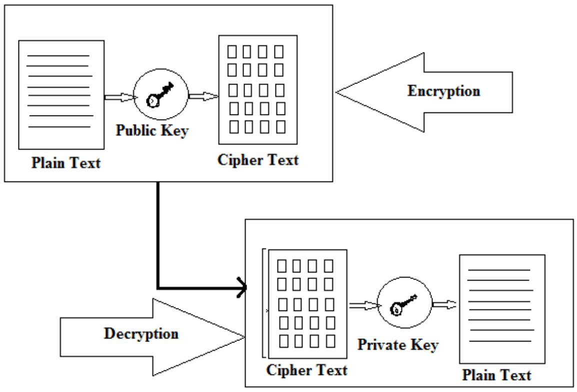

Figure 2: Encryption and Decryption mechanisms [4]

Digital signatures are the electronic equivalent of ordinary signatures in electronic data. Such mechanisms are constructed by properly plying asymmetric encipherment. The decipherment of a data unit with the private key of an entity corresponds to be signature procedure of the data unit. The result of digital signature of the particular data unit produced by the holder of the private key[3].

The access control mechanisms are used to provide access control services. These mechanisms may use the authentication identity of an entity or order to determine and enforce the access rights of the entity. For example – firewalls and operating system access privileges[5].

Traffic-Padding mechanisms provide protection from traffic analysis attacks. Several protocols and security mechanisms include padding mechanisms to protect the exchanged communication.

The routing control mechanisms allow the selection of a specific route for the communicating data, either dynamically or statically through prearranged routes.

Notarization mechanisms are used to assure the integrity, the source or destruction and the time of sending or delivering of transmitted data. Notarization mechanisms may be supported by other mechanisms such as digital signatures, encipherment, or integrity mechanisms[5][6].

3.1 Network Security Attacks

Some basic network security attacks are:-

- Eavesdropping attacks
- Logon abuse attacks
- Spoofing
- Intrusion attacks
- Hijacking attacks
- Denial-of-service (DoS) attacks
- Application-level attacks

3.2 Grid Security Issues

A Grid system is a mechanism to pool resources on demand to improve the overall utilization of the system[10]. The issues and concerns that we had for personal safety, trust, authorization, etc. are important issues for grid computing systems as well[14]. The Grid system requires a monitoring system in place to monitor the resource usage, trust management system to create, negotiate, and manage trust between other systems or "strangers", and authorization system to authorize the users to a access certain set of resources.

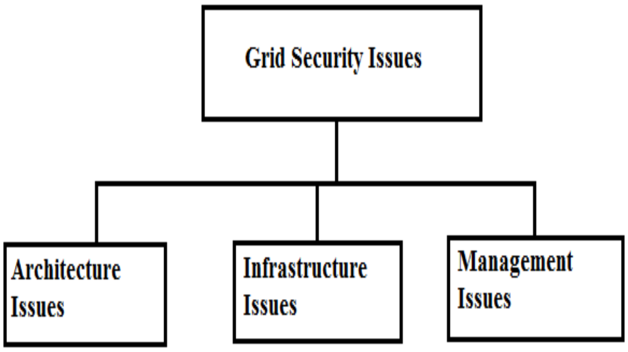

Figure 3: Grid Security Issues [16]

Architecture Issues

This issue addresses concerns pertaining to the architecture of the Grid. Mainly architecture issues can be categorized under three parts[16]. These are:

- Information Security
- Authorization
- Services

We categorized these requirements under information security. Similarly resource level authorization is a critical requirement for Grid systems. Finally, there are issues where users of the Grid systems may be denied the service of the Grid or the Quality-of-Service (QOS) is violated[5].

Infrastructure Related Issues

This issue relates to the network and host components which constitute the Grid infrastructure[11]. Host level security issues are those issues that make a host apprehensive about affiliating itself to the Grid system[13][17]. The main sub issues are –

- Data protection
- Job starvation
- Host availability

4. NETWORK SECURITY RISK & CHALLEGES

We analyzed lots of responses to strategies security survey from IT and security pros at companies whose use Grid computing infrastructure, and we found that they take information security every bit as seriously as large enterprises. They are wrestling with the same challenges, including managing the complexity of security, enforcing policies, preventing data breaches, and assessing risk, but they are doing it with less funding, expertise, and technology[15][18]. Here, we discuss about two types of problems:-

- Managing Security Complexity
- Enforcing Policy

Managed and hosted security services are arguably the only plausible way to cost-effectively counter security complexity. The trick is finding the right one. We discuss exactly how to choose a best security services strategies for Grid computing environments, which includes a checklist tailored to low, medium and high risk environments. Integrated security suite provides desktop and server antivirus and antimalware protection as well as email and web security, all with unified management. Then fill in gaps by adding such services as endpoint data loss prevention and encryption, which increasingly is recruitment for state data privacy laws. Of course, the best security can be bypassed if you don't have a strong password policy.

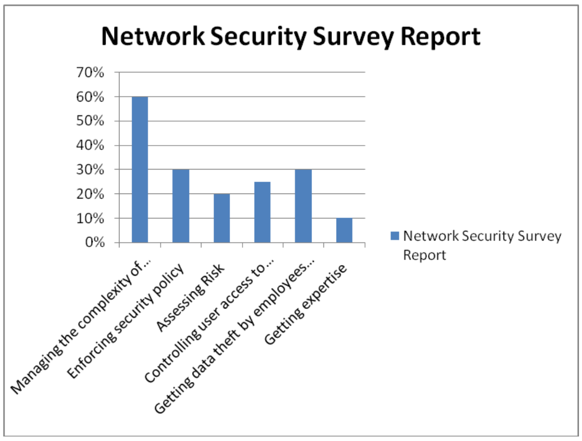

Figure 4: Network security survey report in 2011

Outsourcing a security technology and management doesn't absolve to responsibility for employee behavior[12][18]. The formulating rules for Grid computing and handling of access to sensitive data takes time, executive buy-in, and some level of automation. Complement education with strong change management policies and procedures to assure that network devices, critical servers, and firewalls are properly configured.

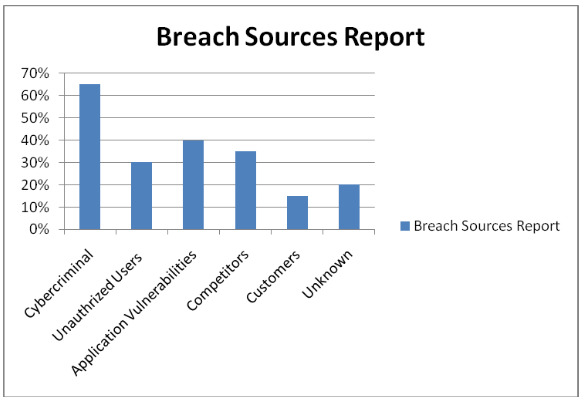

Figure 5: Sources of breaches report in 2011

5. CONCLUSION

The issues and concerns with Grid Computing such as personal safety, trust, authorization, etc. are important issues for Grid systems. The Grid system requires a monitoring system in place to monitor the resource usage, trust management system to create, negotiate, and manage trust between other systems or "strangers", and authorization system to authorize the users to a access certain set of resources. Also, we analyzed lots of responses to strategies security survey from IT and security pros at companies whose use Grid computing infrastructure, and we found that they take information security every bit as seriously as large enterprises. They are wrestling with the same challenges, including managing the complexity of security, enforcing policies, preventing data breaches, and assessing risk, but they are doing it with less funding, expertise, and technology.

6. REFERENCES

[1] McNab, Chris, Ed., "Network security assessment", 2004, 005.8,323268

[2] Dr. Ion PETRE, Department of IT, Åbo Akademi University, http://www.abo.fi/~ipetre/

[3] Markus Jocobsson, Moti yung, "Applied Cryptography and Network Security", 2004.

[4] Cryptography and Network Security, available at http://web.abo.fi/~ipetre/crypto/

[5] Stallings, william, "Network security essentials: applications and standards", 2002, 658.478, 293400

[6] Computer Networks and the Internet, Available at http://www.cse.cuhk.edu.hk/~cslui/ceg4430_lecture.html

[7] Lecture Notes on Computer and Network Security, Available at http://cobweb.ecn.purdue.edu/~kak/ compsec/Lectures.html

[8] Bode, Hendrik W, "Network analysis and feedback amplifier design", 1956, 621.3421, 17942

[9] Weinberg, Louis, "Network analysis and synthesis", 1962, 621.3815, ECD763

[10] Anderson, Brian D.O.; Vongpanitlerd, Sumeth, "Network analysis and synthesis : a modern systems theory approach", 1973, 621.3815, ECD181

[11] Zobrist, George W., "Network computer analysis", 1969, 621.38172, ECD159

[12] Kulshreshtha, Alok; Singh, Prashant Kumar; Choudhary, Sachin Kumar, "Network management through mobile agent", 2001, 621.38072, ECDB43

[13] Kou, Weidong, "Network security and standards", 1994, 621.3891, ECD1008

[14] Mathur, Anoorag; Lal, Dhananjay; Narula, Puneet, "Network security and TCP performance enhancement in mobile environment", 1999, 621.38072, ECDB75

[15] McNab, Chris, Ed., "Network security assessment", 2004, 005.8,323268

[16] Stallings, william, "Network security essentials: applications and standards", 2002, 658.478, 293400

[17] Durr, Michael, "Networking ibm pcs", 1993, ECD732G

[18] Neil Roiter, “Midmarket Security: Risk and Responses” April 2011