3 Taxonomy of Grid Security Issues

3.1 Introduction

When I started to write this book, one long time memory came rushing back. This was the period of my life which I really cherish. It was the period during my college days. During those days we used to travel long-distances by pooling together the vehicles we had. We had lots of wonderful experiences during that time which can itself be a topic of a book. Pooling helped us in optimizing the resources for every trip based on the number of people traveling and the distance to be traveled. However, it was a source of anxiety for us also. Whenever I gave my car to the pool I was worried about the car because it may not always be handled with care. In addition, we always used to have a few people for the trip who were complete strangers to me. Therefore, trust was a real issue. On the other hand, when I traveled in somebody else's car I felt anxious about my safety as most of our vehicles were at least a few decades old. My anxiety did not end here. After every trip, I used to lose a few of my favorite cassettes, CDs, books, or some of my other "valuable" possessions. Though, I am mentioning some of the anxieties of the trips, I loved them and looked forward to them. We did have our share of weird incidents. Like the one where we ran out of gas and were stranded in the middle of a desert. We also once got stranded after our keys got stolen in a hotel room. After a few of those incidents, we learnt to cope with them. We regularly used to *monitor* the gas usage of the cars, hand over the keys only to *authorized* valets, used some sort of "trust" mechanisms before inducting strangers into the group, a store for valuables with key with one of us, a check up of the vehicles to be used for the trips, and several other such mechanisms. Once these mechanisms were implemented the journey and the trip became more enjoyable as we spent time enjoying the trip rather than worrying about mundane affairs.

Once I started writing this book, I noticed an uncanny similarity between our college carpooling mechanisms and the grid system. Similar to the car pooling system, a grid system also is a mechanism to pool resources on-demand to improve the overall utilization of the system. Similarities do not end here also. The issues and concerns that we had for personal safety, trust, authorization, etc. are important issues for grid computing systems as well. For example, similar to the car pooling system where we were concerned about cassettes and CDs, in grid systems also one is concerned about the data processed. Moreover, the concerns of a user donating his/her host to the grid system are very similar to the concerns I had about my car. Similar to the car pooling system, the grid system also 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 an authorization system to authorize the users to a access certain set of resources. In this chapter we will briefly talk about the different security issues and solutions in the grid system. However, this chapter is not meant to be comprehensive as all the components will be elaborated upon in the course of the book. This chapter would provide an overall landscape so that readers can choose the issues they are interested in.

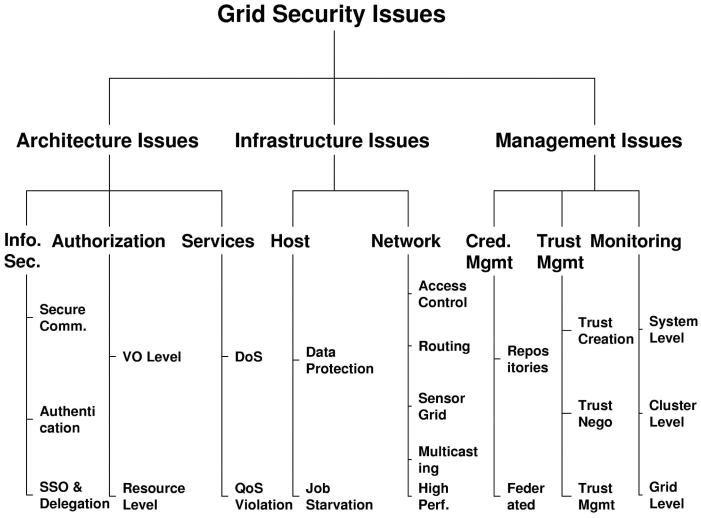

Fig. 3.1. Taxonomy of grid security issues

3.1.1 Grid Security Taxonomy

Figure 3.1 shows the categorization of the different security issues in a grid. The grid security issues can be categorized into three main categories: *architecture related issues*, *infrastructure related issues*, and *management related issues*.

Architecture Related Issues

These issues address concerns pertaining to the architecture of the grid. Similar to car pooling, where we were concerned about our cassettes and CDs, users of the grid are concerned about the data processed by the grid and hence there is a requirement to protect the data confidentiality and integrity, as well as user authentication. We categorize 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 system may be denied the service of the grid or the Quality-of-Service (QoS) is violated. These fall under the purview of service level security issues.

Infrastructure Related Issues

These issues relate to the network and host components which constitute the grid infrastructure. Host level security issues are those issues that make a host apprehensive about affiliating itself to the grid system. The main subissues here are: data protection, job starvation, and host availability. A grid involves running alien code in the host system. Therefore, the host can be apprehensive about the part of the system which contains important data. Similarly, a host can also be concerned about the jobs that it is running locally. The external jobs should not reduce the priority of the local jobs, and hence lead to job starvation. Similarly, if the host is a server, it can be concerned about its own availability. There should be mechanisms to prevent the system from going down resulting in denial-of-service to the clients attached to the host.

Management Related Issues

The third set of issues pertains to the management of the grid. Managing credentials is absolutely important in grid systems because of the heterogeneous nature of the grid infrastructure and applications. Like any distributed system, managing trust is also critical and falls under the purview of management related issues. Similar to the car pooling case where monitoring of gas was mandated, grid systems also require some amount of re-

source monitoring for auditing purposes. Much of the information obtained from the monitoring systems is fed back to higher level systems like intrusion detection and scheduling systems.

3.2 Architecture Related Issues

Architecture level issues address the concern of the grid system as a whole. Issues like Information security, authorization, and service level security generally destabilize the whole system and hence an architecture level solution is needed to prevent those. In this section we will briefly touch upon the issues and some solutions.

3.2.1 Information Security

We define information security as the security related to the information exchanged between different hosts or between hosts and users. The concerns at the information security level of the grid can be broadly described as issues pertaining to *secure communication*, *authentication*, and issues concerning *single sign on and delegation*. Secure communication issues include those security concerns that arise during the communication between two entities. These include confidentiality and integrity issues. Confidentiality indicates that all data sent by users should be accessible to only "legitimate" receivers, and integrity indicates that all data received should only be sent/modified by "legitimate" senders. There are also issues related to authentication, where the identities of entities involved in the overall process can be accurately asserted. These are critical issues in all areas of computing and communication and become exceedingly critical in grid computing because of the heterogeneous and distributed nature of the entities involved there. In addition to the secure communication features users are also concerned about single sign on capability provided by the grid computing infrastructure. In single sign on the authentication is done once.

The information security issues exist in all fields of computing and communications and have been studied for quite some time. In the grid computing area, the researchers and practitioners have come together to create the Global Grid Forum (GGF) (now called OGF). They have released an open standard called Open Grid Standards Architecture (OGSA). There is a Grid Security Infrastructure (GSI) layer of OGSA which addresses most of the information security challenges mentioned above. The

Globus toolkit is an open source implementation of OGSA. Details about grid information security are provided in Chap. 4.

Solutions to Information Security Issues

The Grid Security Infrastructure (GSI), developed independently and later integrated as part of the OGSA standards, addresses all the stated architectural concerns. GSI is based on proven standards such as public key encryption, X.509 certificates, and the Secure Sockets Layer (SSL) and enables secure authentication and communication over computer networks. The latest version of the GSI based on Globus Toolkit 4.0 also allows Web services based security. Please see details provided in Chap. 4.

- **Secure Communication:** The GSI uses public key cryptography, as the basis for creating secure grids and SSL/TLS for data encryption. In public key cryptography, the entities generate public/private key pairs based on some cryptographically secure mathematical function. A message when encrypted by the public key can only be decrypted by the private key corresponding to the public key. The public keys are known to everyone.
- **Authentication:** A central concept in GSI authentication is the *certificate.* Every user and service on the grid is identified via a certificate, which contains information vital to identifying and authenticating the user or service.
- **Single Sign on and Delegation:** The GSI provides a single sign on and delegation capability, which reduces the number of times the user must enter his/her pass phrase when multiple resources are used, which is common in a grid scenario. This is done by creating a proxy. A proxy consists of a new certificate (with a new public key in it) and a new private key. The new certificate contains the owner's identity, modified slightly to indicate that it is a proxy. The new certificate is signed by the owner, rather than a Certification Authority (CA). The certificate also includes a time notation after which the proxy should no longer be accepted by others.

3.2.2 Authorization

Another important security issue is that of authorization. Like any resource sharing system, grid systems also require resource specific and system specific authorizations. It is particularly important for systems where the resources are shared between multiple departments or organizations, and

department wide resource usage patterns are pre-defined. Each department can internally have user specific resource authorization also. The authorization systems can be mainly divided into two categories: *VO Level Systems* and *Resource Level Systems*. Virtual Organization or VO level systems have a centralized authorization system which provides credentials for the users to access the resources. Resource level authorization systems, on the other hand, allow the users to access the resources based on the credentials presented by the users.

Grid Authorization Solutions

Several authorization systems can be applied to the grid context.

- **VO Level Systems:** VO level grid authorization systems are centralized authorization for an entire Virtual Organization (VO). These types of systems are necessitated by the presence of a VO which has a set of users, and several Resource Providers (RP) who own the resources to be used by the users of the VO. Whenever a user wants to access certain resources owned by a RP, he/she obtains a credential from the authorization system which allows certain rights to the users. The user presents the credentials to the resource to gain access to the resource. In this type of systems, the resources hold the final right in allowing or denying the access to the users. Examples of VO level grid authorization systems are Community Authorization Service (CAS) Virtual Organization Membership Service (VOMS), and Enterprise Authorization and Licensing System (EALS).
- **Resource Level Systems:** Unlike the VO level authorization systems, which provide a consolidated authorization service for the virtual organization, the resource level authorization systems implement the decision to authorize the access to a set of resources. Therefore, VO level and resource level authorization systems look at two different aspects of the grid authorization. In Chapter 5, we have provided details of different resource level authorization Systems like Akenti, Privilege and Role Management Infrastructure Standards Validation (PERMIS), and the GridMap system.

3.2.3 Service Security

One of the most important security threats existing in any infrastructure is the malicious service disruption created by adversaries. Many such exam-

ples exist in the Internet space where servers and networks are brought down by a huge amount of network traffic and users are denied the access to a certain Internet based service. Since grid computing deployment has not reached the "critical mass" yet, the service level attacks are also currently nonexistent. However, with the grid computing poised for a huge growth in the next few years, this area should be looked upon with utmost concern by the grid security experts. The grid service level security issues can be further subdivided into two main types: *QoS Violation Issues* and *Denial-of-Service (DoS)* related issues. The first issue is about the forced QoS violation by the adversary through congestion, delaying or dropping packets, or through resource hacking. The second one is more dangerous where the access to a certain service is denied. More details about the attacks and solutions are provided in Chap. 6.

Solutions to Service Attacks

It is to be noted that the DoS attacks and QoS violation attacks are research topics for researchers in the areas of networks, services, and operating systems. In Chap. 6, we provide an overview of different research efforts that are being undertaken and the solutions that have been proposed.

- **DoS Solutions:** The solutions proposed for Denial-of-Service (DoS) attacks can be categorized into mainly two types: *preventive* solutions and *reactive* solutions. Preventive solutions try to prevent the attack from taking place by taking precautionary measures. Reactive solutions, on the other hand, react to a DoS attack and are generally used to trace the source of the attack. Some examples of preventive solutions are filtering, throttling, location hiding, and intrusion detection. Examples reactive solutions include logging, packet marking, Link testing, and others.
- **QoS Violation:** This is an active area of research and several architecture and solutions have been proposed. Most of these solutions rely on some amount of monitoring and metering systems which try to detect the QoS levels of the systems and then make decisions to raise the alarms. The WATCHERS project is an example of such a system. More details of this project and a grid accounting system are provided in Chap. 6.

3.3 Infrastructure Related Issues

A grid infrastructure consists of grid nodes and the communication network. The security issues related to the grid infrastructure are also of paramount importance.

3.3.1 Host Security Issues

Host level security issues are those issues that make a host apprehensive about affiliating itself into the grid system. The main subissues here are: data protection and job starvation. Whenever a host is affiliated to the grid, one of the chief concerns is regarding the protection of the already existing data in the host. The concern stems from the fact that the host submitting the job may be untrusted or unknown to the host running the job. To the host running the job, the job may well be a virus or a worm which can destroy the system. This is called the *Data protection issue*. *Job starvation* refers to a scenario where jobs originating locally are deprived of resources by alien jobs scheduled on the host as part of the grid system.

Solutions to the Host Security Issues

Several solutions have been proposed for data protection and job starvation issues.

- **Data Protection:** Solutions in this space use isolation to restrict the data to the grid or external applications. In Chap. 7 we discuss several isolation techniques *viz.* application level sandboxing, virtualization, and sandboxing. The first type of solution is through the use of proof carrying code (PCC) where the code generators generate proofs of application safeness and embed those in the compiled code. The second solutions looks at creating Virtual Machines (VM) on the physical machine resulting is strong isolation properties. The third type of solution, or the sandboxing solutions, traps system calls and sandboxes the applications to prevent them from accessing data and memory based on certain policies.
- **Job Starvation:** Different solutions which look at the problem of job starvation can be categorized as *advanced reservations* and *priority reduction* techniques. Under advanced reservation system, a user requests a set of resources (can be CPU, memory, disk space, etc.) for a specified amount of time for the set of

jobs to be run. The resources are booked based on the availability, security, QoS and other metrics. Once the resources are booked, the resource providers honor the contract and have every right to terminate the job once the contract expires. These techniques require schedulers to work hand-in-hand with the resources/hosts providing service to the end users. Priority reduction techniques, on the other hand, reduce the priorities of the long running jobs to reduce the possibility of starvation. Most of the solutions in this space are ad hoc in nature and look at specific solutions

3.3.2 Network Security Issues

In the context of grid computing, network security issues assume significant importance mainly due to the heterogeneity and high speed requirements of many grid applications. Moreover the grid inherits some of the generic network issues also. *Access control and isolation* are important requirements for traffic flowing through the grid networks. In this area, integration of grid technologies with VPN and firewall technologies assume significance. *Routing* of packets in networks based on routing tables is a specific network issue. Attacks in routing include link and router attacks which may cause significant destruction. Many of the issues still require research attention. *Multicasting* is an efficient means of information dissemination and may assume importance for grid networks in the future. Member authentication, key management, and source authentication are specific security issues in multicasting. Another topic of interest in grid networks is the integration of *sensor networks* with grid technologies. Several sensor network attacks like sybil attacks, wormhole, and sinkhole attacks, node hijacking, need to be tackled before the sensor grid vision can get realized. Finally, there are security issues in high performance interconnects.

Solutions to the Grid Network Issues

Many of the grid network issues are active areas of research where solutions are mostly developed in labs and not yet commercialized. In Chap. 8, we have included the research activities in many of these areas.

- **Access Control & Isolation:** Many of the grid and Web services solutions cannot work effectively with firewalls and virtual private networks (VPN) which have become ubiquitous in

today's enterprises. The area requires significant research efforts. Some of the research efforts like Adaptive Grid Firewalls (AGF) and Hose have been included in Chap. 8.

- **Secure Routing:** This area of research is inherited from the traditional networking area. Most routing protocols use digital signatures and passwords for message exchange which do not solve the advanced attacks like source misbehavior. More research is needed in this area. Some topics like inconsistency detection are briefly touched upon in our discussion in Chap. 8.
- **Secure Multicasting:** This has been an active area of research for the last few years. Most of the solutions presented in this area are research outputs and rarely implemented in a large scale. However solutions like centralized and hierarchical member authentication systems, tree-based, and core based key management systems, and stream signing, and chaining type solutions are important and require mention. Details of the different techniques are provided in Chap. 8.
- **Sensor Grids:** Security in sensor networks is a very important issue due to the computational constraints imposed by the devices and network and bandwidth constraints. This is also an active area of research and several solutions have been proposed like SPINS and TinySec.
- **High Speed Networks:** One of the most important issues in the adoption of security solutions is performance. A security solution which requires firewall/intrusion detection, encryption/decryption, message authentication, distributed denial of service (DDoS) attack protection, etc. results in a significant overhead which significantly reduces the performance. We have discussed some hardware based solutions like CYSEP and protocol level solution like Infiniband Security in Chap. 8.

3.4 Management Related Issues

If we go back to the car pool example, we find that management was necessary there. Similarly, the grid management is important as the grid is heterogeneous in nature and may consist of multiple entities, components, users, domains, policies, and stake holders. The different management issues that grid administrators are worried about are credential management, trust management, and monitoring related issues.

3.4.1 Credential Management

Management of *credentials* becomes very important in a grid context as there are multiple different systems which require varied credentials to access them. Credential management systems store and manage the credentials for a variety of systems and users can access them according to their needs. This mandates for specific requirements from the credential management systems. For typical grid credential management systems mechanisms should be provided to obtain the initial credentials. This is called the *initiation* requirement. Similarly, secure and safe *storage* of credentials is equally important. In addition, the credential management systems should be able to access and renew the credentials based on the demand of the users. A few other requirements which are important for grid systems are *translation*, *delegation*, and *control* of the credentials. Based on the above requirements, credential management systems are mainly of two types: *credential repositories* or credential storage systems, and *credential federation systems* or credential share systems. The first set of systems are responsible for storing credentials while the second set of systems are responsible for sharing credentials across multiple systems or domains.

Different Credential Management Systems

Different types of credential repositories and credential federation systems have been developed. In Chap. 9, we provide a detailed account of some of the important systems which are useful from the grid context. The two systems are not competitive, rather complementary in nature.

- **Credential Repositories:** The basic purpose of credential repositories is to move the responsibilities of credential storage from the user to these systems. Some of the examples of credential repositories are smart cards, virtual smart cards, and MyProxy Online Credential Repositories. Smart cards are credit card sized tokens which contain the secret keys of the users. These are extremely secure, however they are expensive. Virtual smart cards embed the features of smart cards in the software where the keys never leave the user's system. MyProxy is a popular implementation of credential repositories specifically for grid systems.
- **Credential Federation Systems:** These systems, protocols, and standards are used for managing credentials across multiple systems, domains, and realms. A few of the examples in this space include VCMan, which is a specific solution for grid and Community Authorization Service (CAS) for inter-operability across

multiple domains. KX.509 is a protocol which provides interoperability between X.509 and Kerberos systems. A standard called the Liberty Framework has been developed by a consortium of 150 companies for creating and managing federated identities. Another popular open source solution in this space is Shibboleth.

3.4.2 Trust Management

Another important management issue which needs to be addressed is the issue of managing trust. Managing trust is not unique to digital or computing systems; it is used everyday and in every sphere of life. Trust is a multi-dimensional factor which depends on a host of different components like reputation of an entity, policies, and opinions about the entity. Managing trust is crucial in a dynamic grid scenario where grid nodes and users join and leave the system. Therefore, there must be mechanism to understand and manage the trust levels of systems and new nodes joining the grid. The trust life cycle is composed of mainly three different phases: *trust creation phase*, *trust negotiation phase*, and *trust management phase*. The trust creation phase generally is done before any trusted group is formed, and it includes mechanisms to develop trust functions and trust policies. Trust negotiation, on the other hand, is activated when a new untrusted system joins the current distributed system or group. The third phase, or the trust management phase, is responsible for recalculating the trust values based on the transaction information, distribution or exchange of trust related information, updating and storing the trust information in a centralized or in a distributed manner.

Trust Management Solutions

Trust management is an active area of research and several trust management systems have been proposed and implemented in a limited manner in the labs of different universities. The main characteristics of trust management systems are scalability, reliability, and security. In other words, the trust management systems should scale in terms of message overheads, storage, and computational overheads, should be reliable in face of failures, and should be secure against masquerade attacks, collusion, and sybil attacks. The different trust management systems can be broadly categorized into reputation based and policy-based trust management systems.

- **Reputation Based:** These types of systems are based on trust metrics derived from local and global reputation of a system or an en-

tity. As part of the discussion in Chap. 10 we discuss the different reputation-based systems including PeerTrust, XenoTrust, NICE, Secure Grid Outsourcing (SeGO) systems.

- **Policy Based:** In policy based systems, the different entities or components constituting the system, exchange and manage credentials to establish the trust relationships based on certain policies. The primary goal of such systems is to enable access control by verifying credentials and restricting access to credentials based predefined policies. These types of system create a policy based trust language. Examples of such systems are PeerTrust Trust Negotiation and TrustBuilder.

3.4.3 Monitoring

Monitoring is the third and one of the most crucial management issues that needs to be tackled in a grid scenario. Monitoring of resources is essential in grid scenarios primarily for two reasons. Firstly, different organizations or departments can be charged based on their usage. Secondly, resource related information can be logged for auditing or compliance purposes. The different stages of monitoring are: *data collection*, *data processing*, *data transmission*, *data storage*, and *data presentation*. The data collection stage involves collecting data through different sensors located at different collection points. The gathered data can be static in nature like network topology, machine configuration, or dynamic like CPU and memory utilization, system load, etc. The Data processing stage processes and filters the data based on different policies and criteria from the data collected from the sensors. The Data transmission stage involves the transmission of collected and processed data to the different entities interested. Transmission involves sending the data in a format understood by other parties over a transmission medium, for example the network. There may be a need for storage of gathered or processed data for future references which is carried out in the data storage stage. Finally, the data presentation stage presents the data in a format understood by the different interested entities.

Different Monitoring Systems

Different monitoring systems available can be broadly categorized into system based, cluster based, and grid based monitoring systems. In Chap. 11, we provide details of different monitoring systems.

- **System Level:** The system level monitors collect and communicate information about standalone systems or networks. For network monitoring Simple Network Management Protocol (SNMP) is an example for managing and monitoring network devices. Examples of open source and popular system monitoring tools include Orca, Mon, Aide, Tripwire, etc.
- **Cluster Level:** The cluster level monitoring systems generally are homogeneous in nature and require deployment across cluster or a set of clusters for monitoring purposes. Popular examples of cluster level monitoring systems include Ganglia from University of Berkeley and Hawkeye from University of Wisconsin Madison.
- **Grid Level:** Grid level monitoring systems are much more flexible than other monitoring systems and can be deployed on top of different other monitoring systems. Many of the grid level monitoring systems provide standards and interfaces for interfacing, querying, and displaying information in standard formats. Examples of such monitoring systems include R-GMA, Globus Monitoring and Discovery Systems (MDS), Management of Adaptive Grid Infrastructure (MAGI), and GlueDomains. R-GMA combines the grid monitoring and information services with relational models. MDS is a Globus component for monitoring and discovering resources while MAGI is a grid management and monitoring system. GlueDomains is used mainly for network monitoring. Details of the different systems are available in Chap. 11.

3.5 Chapter Summary

Grid computing is an interesting and a high potential solution for most enterprises. However, security is one of the major impediments in widespread grid adoption. In this chapter we have provided a high level taxonomy of the grid systems. We have categorized the issues pertaining to grid computing security into three main buckets *viz.*, architecture related issues, infrastructure related issues, and management related issues. Architecture related issues are concerned with the overall architecture of the grid system like the concerns pertaining to the information security, concerns about user and resource authorization, and issues pertaining to the overall service offered by the grid system. The infrastructure related issues are concerned with the underlying infrastructure which include the hosts or the machines, and the network infrastructure. In addition, several management systems need to be in place for an all pervasive enterprise level and secure grid sys-

tems. There are three main types of management systems which are important from the grid perspective namely the credential management systems, the trust management systems, and the monitoring systems. All the three issues mentioned above are dealt with in this book along with existing solutions and potential concerns. In the next chapter, we will look at the Grid Information security architecture mainly from the perspective of the Grid Security Infrastructure (GSI) and its open source and popular implementation, the Globus toolkit.

http://www.springer.com/978-3-540-44492-3

Grid Computing Security
Chakrabarti, A.
2007, XIV, 331 p., Hardcover
ISBN: 978-3-540-44492-3