MANAGING SECURITY OF GRID ARCHITECTURE WITH A GRID SECURITY OPERATION CENTER

Julien Bourgeois and Raheel Hasan
Computer Science Laboratory (LIFC), University of Franche-Comte (UFC)
1 Cours Leprince-Ringuet, 25201 Montbeliard, France

Keywords: Grid security, Grid security operation center, Specificities of grid networks.

Abstract: Due to the nature of grid computing networks, security pitfalls are plethora and adversaries are sneaking to launch attacks. Keeping this scope in mind, we will discuss our proposed solution for securing grid computing networks that we have called gSOC (Grid Security Operation Center). The main advantage of gSOC is that it can give a global view of security of the entire grid infrastructure. The main difficulty is to deal with the specificities of grid infrastructure, that are: multi-sites networks, multi-administrative domains, dynamic collaboration between nodes and sites, high number of nodes to manage, no clear view of the foreign networks and exchange of security information among different domains.

1 INTRODUCTION

The industrial and scientific communities are always looking for more computational power to achieve this goal researchers have studied multiple solutions for interconnecting organizations in order to share computational resources, which has given birth to grid networks.

There exist multiple definitions of a grid network but in the rest of this article we will only consider the following one. We define a grid network as a network of multiple administrative domains where each administrative domain consists of multiple network sites which put a service (storage space, computational resource, etc.) at disposal of users. An administrative domain is an entity which follows homogeneous security policy through all its sites. According to the above definition a grid network may be composed of a high number of computational devices across the globe. A grid system is interfaced with its users through a middleware. There are different grid middlewares such as gLite (gli), Unicore (Uni), ARC (kno) or Unibus (Dawid Kurzyniec and Sunderam., 2007). The largest grid service in Europe is EGEE (enabling grid for e-sciences) (ege) which is based on gLite software. EGEE connects many local grids from different countries for example, Germany DE-Grid, Netherlands BIG-Grid or Belgium BE-grid. It process around 300,000 jobs per day from scientific domains ranging from biomedicine to fusion science. Grid networks are therefore composed of different administrative domains that are often located in different countries. They have different security policies and they must respect possibly different laws in each country. This heterogeneity arise issues in the security management of grid networks which are not taking into account by existing middleware or security management softwares. Therefore, these properties that makes grid networks special in regard to multipurpose networks which have to be taken into account by security environment, like:

1. Grid network structure with different administrative domains, each of them composed of multi-sites networks.
2. High number of nodes which collaborate with each other dynamically.
3. View of security events of foreign networks unavailable.

To cope with these issues, we have designed gSOC (Grid Security Operation Center) whose aim is to give a global view of security of a grid network by taking into account its specificities. Section 2 presents our proposed architecture named gSOC. Section 3 concludes this article and announces some future works.

Bourgeois J. and Hassan R. (2009).
MANAGING SECURITY OF GRID ARCHITECTURE WITH A GRID SECURITY OPERATION CENTER.
In *Proceedings of the International Conference on Security and Cryptography*, pages 403-408
DOI: 10.5220/0002188304030408

2 PROPOSED ARCHITECTURE: THE gSOC ENVIRONMENT

2.1 Introduction

gSOC is a security operation center dedicated to grid computing networks. In grid networks, there is no mechanism for sharing security information with multiple administrative domains which consists of multiple sites. Therefore in grid networks handling of cross domain attacks and their expansion is very difficult. Attacks launched by grid users with massive grid computational power and memory could be more powerful than normal attacks. By considering the above parameters, the need of gSOC is mandatory. gSoc also provides a better mechanism for trust management within multiple administrative domains connected to the grid.

At present gSOC design is under the development phase, we started our work by keeping the target to provide better trust management and sharing of security information between multiple administrative domains.

2.2 The Components of the gSOC Environment

gSOC is composed of five components partly based on the CIDF specifications (Staniford-Chen et al., 1998), from bottom to top: data collectors (CBoxes), remote data collectors (R-CBoxes), Local Analyzers (LAs) and a Global Analyzer (GA) and Secure Virtual Organization (SVOBox).

2.2.1 Data Collection Box

A CBox collects data from sensors located on the same segment of a network. A sensor can be a host, a server, a firewall, an IDS or any system that generates logs. The advantage of our log collection approach is that no software has to be installed on the sensors. Moreover, our system is compatible with a wide range of hardware and software. A CBox formats logs and sends them to a local intrusion database (lidb). In each site we have one or several CBoxes and one of them acts as a Master CBox (M-CBox). The M-CBox is responsible for the management of all the CBoxes located on the same site. It polls regularly the other CBoxes and when a CBox is down, the M-CBox will collect data on the segment of the failed CBox. Each Master CBox also has a backup which polls it regularly and will become Master if it needs to be.

2.2.2 Remote Data Collector

An R-CBox is a special CBox which collects data coming from some critical sensors and from sensors hosting security tools in any site. Afterward, data is forwarded to the local intrusion database of another site and is analyzed to give in real time the approximate security level of the concerned site. This helps to anticipate a reaction when a critical intrusion occurs or to investigate and troubleshoot a site that could be compromised, even if a hacker erases the logs on the compromised sensors (including the security tools).

2.2.3 The Local Analyzer

A Local Analyzer (LA) is responsible for intrusion detection at any site of a network. It analyzes formatted logs located in a local intrusion database (lidb) and generates alerts. Afterward, it correlates the alerts to find more complex intrusions (intrusions composed of several events, distributed intrusions, intrusions directed to many sensors, etc.). The LA also compress alerts by merging similar ones. All the alerts generated by an LA are sent to the global intrusion database (gidb). The gidb can have a mirror of itself for high availability purpose.

2.2.4 The Global Analyzer

The Global Analyzer (GA) is a chosen LA responsible for the global intrusion detection in a network. It analyzes alerts from the Global Intrusion database (gidb), correlates and merges them if possible to generate optimized outputs. It is also able to detect more sophisticated intrusions that are directed to several sites. The GA regularly polls the other LAs and when one of them is down, the GA detects the occurring intrusion into the concerned site. Another LA acts as the backup of the GA and polls it regularly. When the GA is down, the backup becomes the GA and another backup is elected.

The gSOC architecture is designed bearing in mind that the data flow processed in the different sites of the network is not always homogeneous. Indeed, in some sites, a large amount of data is processed and in this kind of situation, several CBoxes are needed for data gathering.

Even though a single CBox has to be installed on each segment, it is not excluded installing several CBoxes on the same segment when the sensors located in this part of the network are operating under high workloads. In quieter sites, only one CBox can be used to collect data coming from all the sensors.

The gSOC also implements the different types of boxes defined for network intrusion detection systems in (Northcutt and Novak, 2002). However, beside the pure technical aspects involved in such implementations, it is necessary to consider the supervision of an IT infrastructure as a full operational project.

Figure 1 displays the flow of security events among multiple sites which are connected under one administrative domain (AD). These security information contains all the suspected threats which incurred in an AD. The mechanism of security information flow is similar in all the other ADs.

2.2.5 Secure Virtual Organization Box

Secure Virtual Organization Box (SVOBox) job is to collect all the correlated security alerts (SA) generated in different administrative domains (AD) which consists of multiple sites. SVOBox assigns certain security level (SL) value using simple metric for real-time security level evaluation which represents three values indicated in colors (red, orange and green). Green indicates no threat occurring in the network, orange indicates that threats are occurring but not critical at this time and red indicates intrusions are in progress which can lead to critical security problems(Ganame, 2008). In addition to this method we have added another step which will be performed at Global Intrusion Data Base (gidb) of every Administrative Domain (AD). According to this step the gidb deployed in an AD will forward this security information to SVOBox where the SVOBox will assign security level value to each AD (see figure 2) as follows,

- If all the sites having green status in an AD that will be placed in security level 1 which is most secure than SL 2 and SL 3.
- If any one site in an AD having status indicating orange that AD will be placed in security level 2 which is more secure than SL 3.
- If any one site in an AD having status indicating red that AD will be placed in security level 3 which is the least secure level.

After the security level (SL) assignment to all the ADs which are now the part of this grid. Before start sharing the resources every AD of this grid would like to have a global view of the security, for global view they must need to share the security information with other ADs in the grid. To share the security alerts among ADs two methods are employed.

First method is to send security alerts to the administrative domains (ADs) of the different security levels (1,2 and 3). In each AD there exists a gidb which contains three different kinds of security alerts (SA) (see figure 3). From top to bottom, the first section collects security alerts from the lesser secure levels. The middle section is for holding security alerts from its local sites which are residing in the same SL. The third section collects security alerts from the most secure levels. Finally, the last section is used to store alerts which an AD do not want to share with others (private alerts). For example, in figure 3, gidb of AD 3 and AD 4 which are in SL 2 can share their security alerts with AD 1, AD 2 at SL 1, and AD 5, AD 6 at SL 3, whereas AD 3 and AD 4 can share their security alerts using the middle section which is reserved for their local sites security alert information as they lies in the same security level that is SL 2. When security alerts are being shared among ADs the two following fields will be appended with each security alert message:

1. Direction of security alert field which directs the security alert to move in the upper or lower direction depending upon the security level value.
2. Time to Live (TTL) field which is used to define the authorized propagation of the security alert. For example, if AD 1 which is in SL 1, wants to share its security alerts only with ADs of SL 2, it will put an upper direction with a TTL set to 1. The TTL will be decreased when the security alert arrives at SL2 so it will not be propagated till SL 3.

Similarly AD 1 and AD 2 can share security alerts with AD 3, AD 4 and between themselves also. AD 5 and AD 6 can share their security alerts with AD 3, AD 4 respectively. This sharing of security alerts will present an updated global view of security of the entire grid. Now each AD can decide according to its organization policies that sharing of resources can be done with the most or least secured AD. This is the objective which we will going to be achieved by using gSOC, as it gives the global view of the entire grid without sharing of all the data (see figure 3).

The second method, is to allow a remote network administrator to query gidb of other administrative domains. The gidb of an AD will connect with gidb of other AD and the remote network administrators of both the ADs will be allowed to query each others gidb to see the security alerts. After the inspection of security alerts by each network administrator they can decide for the sharing of resources. This solution is also possible but the drawback is that it requires a constant monitoring and constant execution of queries on gidb which is not an efficient solution in case of major attacks like DoS/DDoS attack.

These two kinds of sharing of security information present some advantages and drawbacks, but they can be used alternatively depending on the type of network and number of generated security alerts.

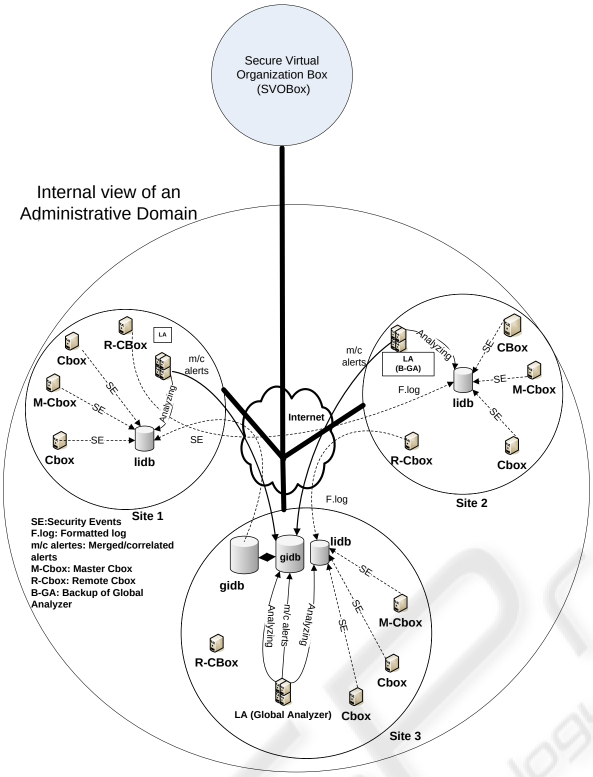

Figure 1: Overview of the internal structure of an Administrative Domain (AD).

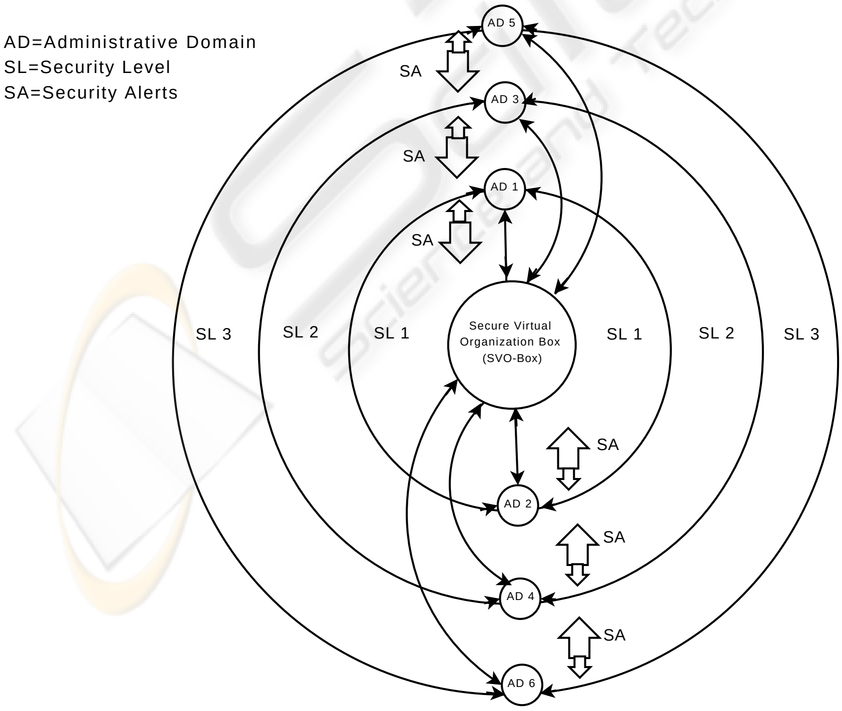

Figure 2: gSOC overview.

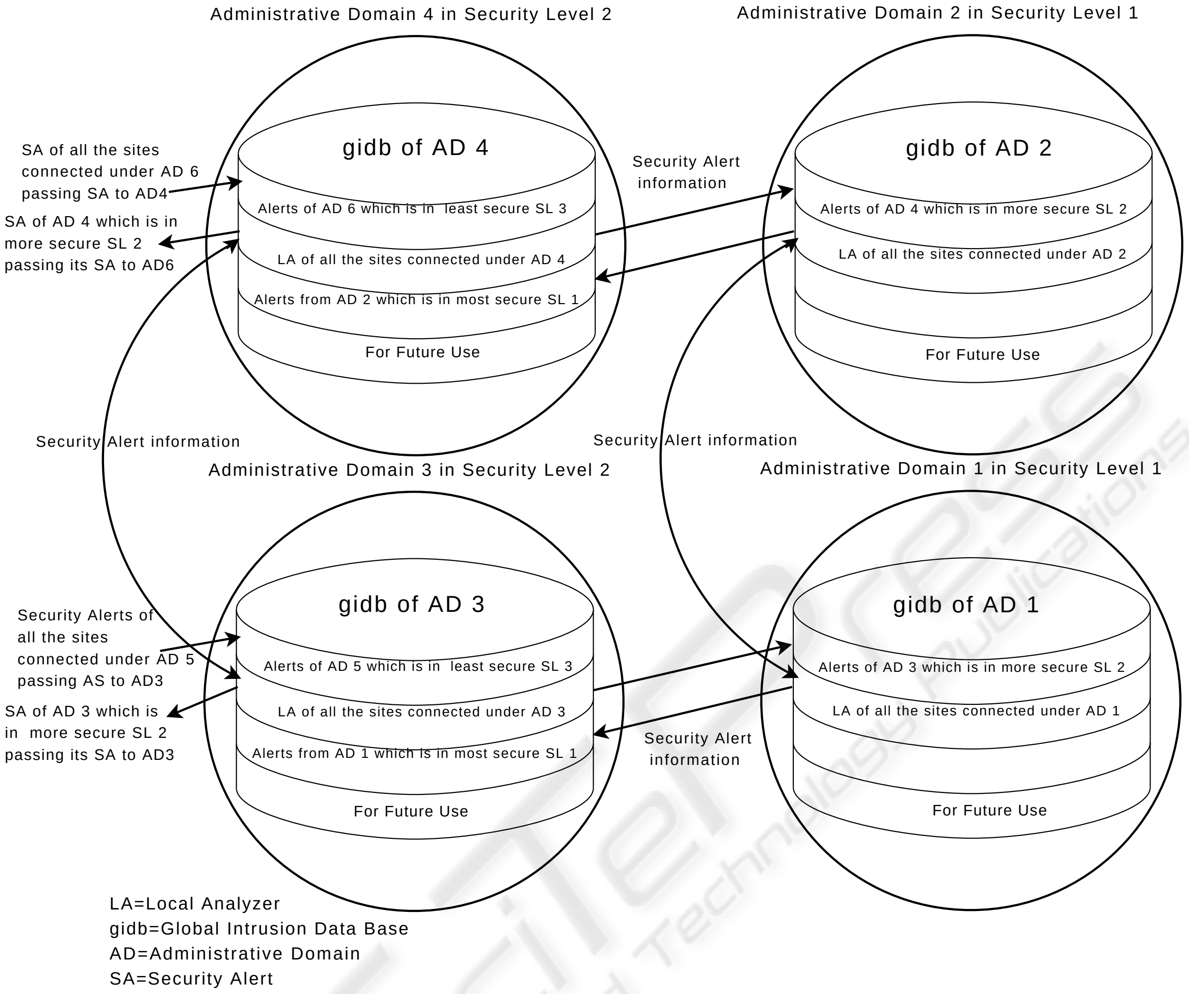
Administrative Domain 4 in Security Level 2
Administrative Domain 2 in Security Level 1
SA of all the sites connected under AD 6 passing SA to AD4
SA of AD 4 which is in more secure SL 2 passing its SA to AD6
gidb of AD 4
Alerts of AD 6 which is in least secure SL 3
LA of all the sites connected under AD 4
Alerts from AD 2 which is in most secure SL 1
For Future Use
Security Alert information
gidb of AD 2
Alerts of AD 4 which is in more secure SL 2
LA of all the sites connected under AD 2
For Future Use
Security Alert information
Security Alert information
Administrative Domain 3 in Security Level 2
Administrative Domain 1 in Security Level 1
Security Alerts of all the sites connected under AD 5 passing AS to AD3
SA of AD 3 which is in more secure SL 2 passing its SA to AD3
gidb of AD 3
Alerts of AD 5 which is in least secure SL 3
LA of all the sites connected under AD 3
Alerts from AD 1 which is in most secure SL 1
For Future Use
Security Alert information
gidb of AD 1
Alerts of AD 3 which is in more secure SL 2
LA of all the sites connected under AD 1
For Future Use
LA=Local Analyzer
gidb=Global Intrusion Data Base
AD=Administrative Domain
SA=Security Alert

Figure 3: Sharing of security alerts using Global Intrusion Data Base (gidb).

2.3 Protecting the Communications between the gSOC Components

One of the key points here is to make sure that no illegitimate computer will act as an LA, a CBox or an R-CBox in order to get privileged access to the system. To ensure the security of our system, any LA or any R-CBox that needs to exchange information with another LA has to use a certificate issued by the network administrator of that AD to prove its identity. Moreover, all the communications between the LAs (also including the GA) and the communications between the R-CBoxes and the LAs will have to pass through an encrypted tunnel, available via the SSL protocol.

3 CONCLUSIONS

The purpose of gSOC is to give a better global view of security without sharing all the data in order to achieve maximum confidentiality. The idea behind gSOC is to give the better tradeoff between confidentiality of security data and having the best possible global view of the network which means sharing all the data. gSOC gives correlated overview by discarding similar information to pass every time, gSOC matches sequence pattern, time pattern, system exposure performance, critical analysis and in final step security policy matching. gSOC does data analysis by correlation, structural analysis and intrusion path analysis. In future experiments we have to check that what is the confidentiality level that can be achievable, the TTL value which needs more study. As LA can be elected to become the gidb in case of failure, in each LA there should therefore have four sections reserved for security alerts.

REFERENCES

http://glite.web.cern.ch/glite/. Lightweight Middleware for Grid Computing.

http://www.eu-egee.org/. Enabling Grids for E-science (EGEE).

http://www.knowarc.eu/. Grid-enabled Know-how Sharing Technology Based on ARC Services and Open Standards (KnowARC).

UNICORE (Uniform Interface to Computing Resources). http://www.unicore.eu/UNICORE.

Dawid Kurzyniec, Magdalena Slawinska, J. S. and Sunderam., V. (2007). Unibus: a contrarian approach to grid computing. *J. Supercomput.*, 42(1):125–144.

Ganame, A.K. Bourgeois, J. (2008). Defining a simple metric for real-time security level evaluation of multi-sites networks. *Parallel and Distributed Processing, 2008. IPDPS 2008. IEEE International Symposium*, 14-18:1 – 8.

Northcutt, S. and Novak, J. (2002). *Network Intrusion Detection*. ISBN: 0-73571-265-4. New Riders, third edition edition. September.

Staniford-Chen, S., Tung, B., and Schnackenberg, D. (1998). The common intrusion detection framework (cidf). In *Information Survivability Workshop*, Orlando.