Protecting Grids from Cross-Domain Attacks Using Security Alert Sharing Mechanism

Raheel Hassan Syed, Maxime Syrame, Julien Bourgeois

Protecting Grids from Cross-Domain Attacks Using Security Alert Sharing Mechanisms[☆]

Syed Raheel Hassan[*], Maxime Syrame, Julien Bourgeois

UFC/FEMTO-ST Institute, UMR CNRS 6174, 1 Cours Leprince-Ringuet, 25201 Montbeliard, France

Abstract

In single administrative domain networks there is only one security policy which can be evaluated by the IT security manager thanks, to monitoring and reporting tools. Grid networks are often composed of different administrative domains owned by different organizations dispersed globally. Such networks are referred to as multi-administrative domain networks. Each domain might have its own security policy and may not want to share its security data with less-protected networks, making it more complex to ensure the security of such networks and protecting them from cross-domain attacks. We propose a Security Event Manager (SEM) called Grid Security Operation Center (GSOC), which facilitate IT security managers in giving a view of the security of the whole grid network without compromising confidentiality of security data. To do so, GSOC provides a security evaluation of each administrative domain (AD) and a parametric security alerts-sharing scheme. Alert sharing can then be tuned in order to meet local security policy rules.

Keywords: Security Management of Grid Computing Networks, Security

[☆]Thanks to: the Laboratory of Computer Science University of Franche-Comte France, Higher Education Commission of Pakistan, Quaid-e-Awam University of Engineering, Sciences and Technology Pakistan for supporting our work financially. Grid'5000 network for providing us the platform to perform tests. Gérard Cécé for verifying the mathematical equations.

[*]Corresponding author. Tel.: +33-381-994787; Fax: +33-381-994791.

Email addresses: raheel.hasan@univ-fcomte.fr (Syed Raheel Hassan), maxime.syrame@edu.univ-fcomte.fr (Maxime Syrame), Julien.Bourgeois@femto-st.fr (Julien Bourgeois)

URL: http://lifc.univ-fcomte.fr/~bourgeoi (Julien Bourgeois)

Alert Sharing, Security Level Assessment, Blocking Cross Domain Attacks, Security Evaluation in Grid Computing Networks.

---

1. INTRODUCTION

1.1. General Security Problems in Computer Networks

In traditional computer networks, it is not recommended to send unencrypted passwords over the network as they can be easily sniffed out by the adversaries. If manually set passwords are weak then there exists many tools that could allow to break them [1, 2, 3]. However usage of manually set password do not preclude the use of strong passwords that would not be easily breakable. The asymmetric-based authentication system is made vulnerable if the attackers use denial-of-service (DoS) attacks on the servers which maintains the certificates and the public/private keys. Most of the time the entire network is compromised from the users that use very simple passwords. Sometimes by the weird security administration that allows the attackers to gain access in the organizations network. The attackers also exploits the vulnerabilities that exist in the applications running in the network [4]. When one or multiple nodes are compromised in a single administrative domain network, it is easy to take quick actions on the hosts and network of the organization to identify the source of the problem. Once the source is identified, new policies and restrictions can be placed within the organization's network to block future threats.

1.2. Specific Security Problems in Grid Computing

For attackers, grid services are very interesting targets to violate quality of service (QoS) by launching DoS and distributed denial-of-service (DDoS) attacks. Section 6.4 of the RFC 3820 [5] mentions there are possibilities for launching DoS attacks on the machines that are responsible for generating key pairs and when granting dynamic delegations using proxy certificates. By the growth of web service and XML technologies in grid computing networks, the application level firewalls are unable to detect sophisticated attacks fabricated using content of the messages [6]. VPNs also struggle to provide end-to-end security as they protect layer 2 or layer 3. When a node in the grid computing gets compromised it is very hard to identify the source of the problem because there are multiple nodes from different administrative domains collaborating with each other. In such cases there is always a high

possibility that attacks could be propagated to other organization's network which are the part of that grid network.

1.3. Proposed Suggestions for Improving the Security of Grid Computing

Keep in mind that 100 percent security is an unrealistic objective [7]. To maintain the security up to maximum, grid computing networks possess Grid Security Infrastructure (GSI) [8] and Public Key Infrastructure (PKI) [9] that uses certificates for validating the legitimate users into the network. However, in [10] Cody et al. envision future research in grid computing will focus on high performance vs high security in grid computing networks because data encryption is inversely proportional to performance. In [11], Schwiegelshohn et al. quoted the example of the XtreemOS [12] project which is using native Linux system-level support for authentication mechanisms (such as PAM, Kerberos and SQL based authentication) instead of a specific middleware based authentication. Their aim is to reduce the complexity of the middleware. They therefore propose security authentication to be shifted to operating systems. Propagation of cross-domain attacks can be blocked if the security information can be shared among the members of the grid computing network [13].

Despite all precautions and propositions, chances still exist that adversaries can target the victim whenever they receive the opportunity. Therefore, there is a high need to have a security monitoring system in place that works in parallel with other security components. It must be scalable and fault-tolerant. It must handle sophisticated network attacks launched using the power of grid networks, must can block cross-domain attacks, must report security breaches in real time, and must share them with other members of the grid computing network. This paper proposes a grid security operation center dedicated for the grid computing networks. The reminder of this paper consists of five sections: a discussion of related work in section 2, an explanation of GSOC design in section 3, a proposition of security evaluation in section 4, a presentation of experiments and results in section 5, and concludes with a proposition of future work in section 7.

2. RELATED WORK

Figure 1 shows the classification of different types of monitoring and security management tools. Kenny and Coghlan [14] proposed **SANTA-G** (Grid-

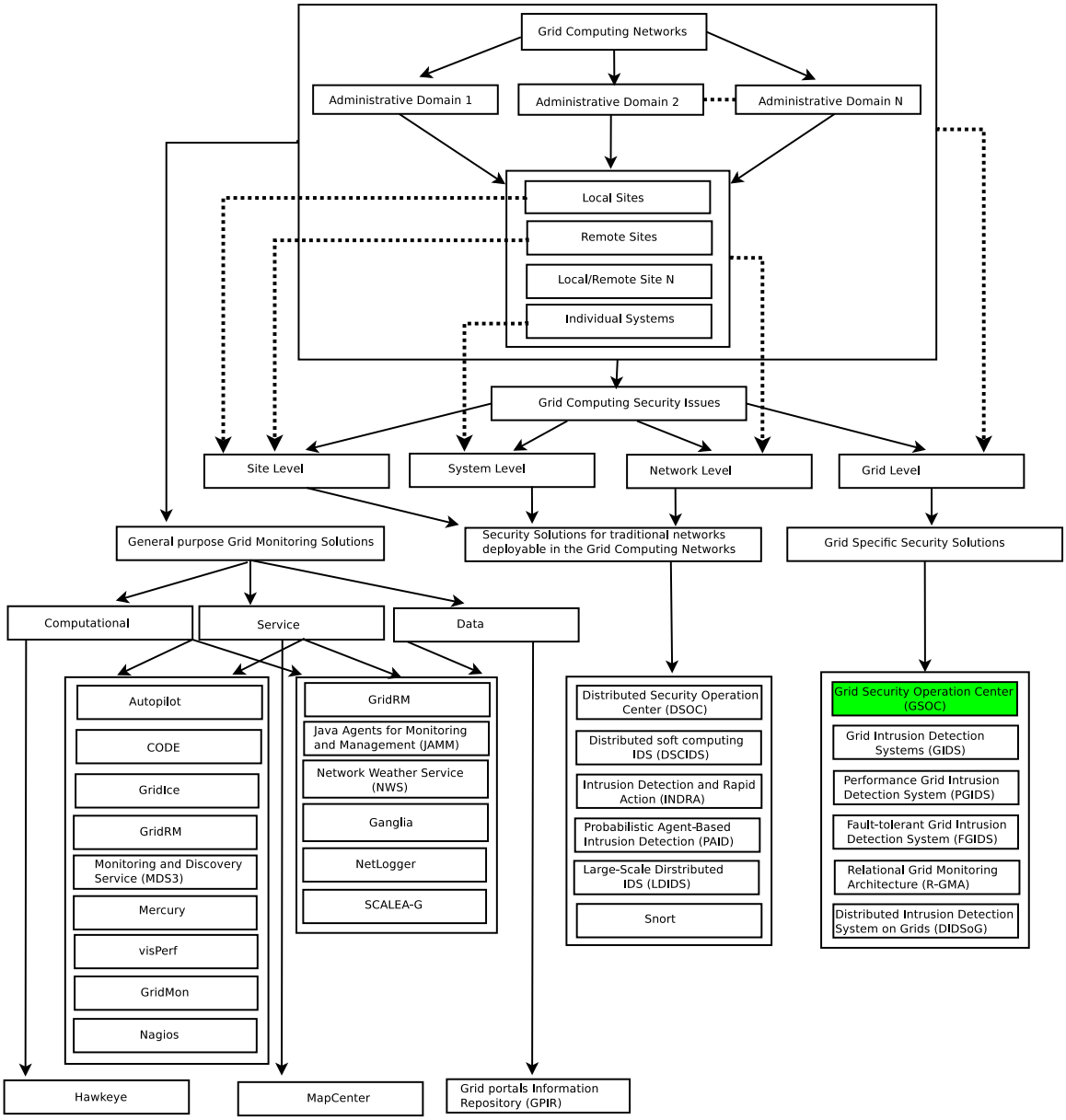


Figure 1: Classification of tools which monitor grid computing networks and security management tools for traditional and grid computing networks.

Enabled System Networks Trace Analysis) which is based on the **RGMA** (Relational Grid Monitoring Architecture), is an implementation of **GMA** which is developed under the European DataGrid (EDG). SANTA-G uses Snort [15] for monitoring network traffic and is composed of three components: **Sensors** that need to be installed on the monitored devices, a **Query Engine**, and a **GUI**. Snort logs suspicious activities that occur in the network. These logs are then forwarded to a SANTA-G sensor which analyzes them and looks for attacks. If a new attack is found, the corresponding log will be sent to the query engine and saved in the database. The query engine publishes the detected attack to its users. The SANTA-G model lacks incident detection, a tracking and response platform, and analysis of reported events to check the patterns for distributed attacks meaning it can not properly detect distributed-denial-of-service-attacks (DDoS). The RGMA has the main database which holds the reported attacks by one or more SANTA-Gs which are running in a grid network. Due to this design limitation, if the size of the network grows rapidly then multiple SANTA-G's begin sending alerts simultaneously making it difficult to hold the alert information for long periods of time. It can, therefore, only correlate reported attacks for a short period of time. This lower its detection capacity for attacks or scans that are using slow-timed pace. SANTA-G only uses Snort as a source of data, giving a restricted view of the network security. SANTA-G does not have a security alert-sharing mechanism and cannot detecting cross-domain attacks.

Fang-Yie Leu et al. proposes three versions of an intrusion detection system dedicated to grid networks: GIDS (Grid Intrusion Detection System), PGIDS (Performance GIDS), and FGIDS (Fault-tolerant GIDS) [16, 17, 18]. All variations of GIDS consist of four types of components: **dispatchers**, which assign network traffic to Detection Nodes (DN) for detecting attacks; **a scheduler** to balance the load between dispatchers; **DN** which use Intrusion Detection System Module (IDSM) for packet analysis and for detecting attacks; and a **Block List Database (BLD)** to hold intrusion information and suspected IP addresses. The objective of GIDS is to detect logical, momentary and chronic attacks. GIDS attack detection accuracy is not very accurate as it does not matches the patterns of similar attacks that occurred in the past by the same attacker. The scope for attack detection is very small [16] since they used TCP, UDP and ICMP flood attacks. To overcome these issues they proposes PGIDS, the objective of PGIDS is to add DoS/DDoS attack detection to GIDS, but PGIDS suffers from DN failure under massive DDoS attacks. A new version, called FGIDS, tackles this problem. The

Table 1: **Comparison of Different Grid Security Management Solutions**

GSS	DoS	DDoS	BF	SAS	SE	Cor	CDA	SC	FT	Comments
GSOC	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Fully Suitable
OSSIM	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Suitable
Prelude [19]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Suitable
DSOC	Yes	Yes	Yes	No	Yes	Yes	No	Yes	Yes	Partially Suitable
Snort	Yes	Yes	Yes	No	No	Yes	No	Yes	Yes	Partially Suitable
R-GMA	Yes	No	Yes	No	No	No	No	No	No	Not Suitable
GIDS	Yes	Yes	No	No	No	No	No	No	No	Not Suitable
PGIDS	Yes	Yes	No	No	No	No	No	Yes	No	Not Suitable
FGIDS	Yes	Yes	No	No	No	No	No	Yes	Yes	Partially Suitable
LDIDS	Yes	?	?	Yes	No	Yes	Yes	Yes	Yes	Not Suitable
DIDSoG	Yes	No	?	Yes	No	Yes	Yes	Yes	Yes	Partially Suitable

GSS=Grid Security Solution, DoS=Denial of Service Attacks, DDoS=Distributed Denial of Service Attacks, BF=Brute Force Attacks, CDA=Cross-Domain Attacks, SAS=Security Alert Sharing, SE=Security Evaluation, Cor=Correlation, CDA=Cross-Domain Attacks, SC=Scalability, FT=Fault Tolerance, ? = Not known.

FGIDS has introduced a new module called Backup Broker to help the scheduler assign another DN to a dispatcher if a massive attacks occurs. FGIDS collects events from multiple sites of an administrative domain, but without having any correlation method for security alerts, it could be vulnerable to DDoS attacks that use grid computing power. Distributed attacks can be detected in one administrative domain but they cannot be detected if they target devices that are located in different administrative domains. More generally, cross-domain attacks cannot be detected by the different versions of GIDS.

The architecture of **Large-Scale Distributed Intrusion Detection System (LDIDS)** proposed by Yonggang et al. [20] is a scalable and fault-tolerant solution. The LDIDS can be applied in grid computing networks due to its modular nature but lacks in the efficiency of the inter communication of its security components. Furthermore, in [20] no details are given about the types of attacks that are detectable by LDIDS.

The Distributed Intrusion Detection System on Grid (DIDoS) proposed by Poula Silva et al. [21] is a hierarchy of multiple intrusion detection systems. The experiments are performed using a grid simulator called Gridsim which can only model and validate the collaboration between the different components of DIDos but not real grid environment conditions. DI-

DoS does not provides a mechanism for sharing alerts between the different administrative domains.

Distributed Security Operation Center (DSOC) proposed by Ganame et al. [22] does not have an intelligent security alert-sharing mechanism between different administrative domains either. Therefore, it cannot detect cross-domain attacks.

Table 1 summarizes the main features of any security management system that handles the security of the grid computing networks. It shows the shortcomings of the security systems that are discussed in this section. In this paper we will discuss GSOC (Grid Security Operation Center) which can overcome the limitations of the discussed solutions.

3. GSOC DESIGN

The GSOC modular design is based on [23][24]. GSOC is composed of seven components namely Event Generating Box (EBox), Logs Collecting Box (CBox), Local Analyzer (LA(DBox+ABox)), Global Intrusion Database (GIDB), Global Analyzer (GA), Remote Logs Collecting Box (RCBox), and Secure Virtual Organization Box (SVOBox). **Figure 5** is a general overview of GSOC architecture and shows the main components of GSOC and their position within the grid network. These components, except SVOBox, are discussed in detail in [13, 25]. In this paper only the short description of these components will be presented.

3.1. Security Alert Generating Mechanism

EBoxes (see figure 2) are the source of data for GSOC and cover a wide range of devices, from a normal computer to any device in the grid computing network. The nice feature is **no additional software is required to be installed on the EBoxes in order to send logs**. GSOC uses only standard logging systems and transport protocol. To integrate a new EBox in GSOC, a simple configuration has to be made like a log redirection. One CBox collects data from multiple EBoxes using standard transport protocols. The logs are processed depending on their protocol and then forwarded to the dispatcher which sends them the to the proper application agent. The application agents extract the information from the logs and create formatted events which are sent to the basic correlation module. One application agent is required for each type of log collected. CBoxes operate at each local site of an Administrative Domain (AD). One CBox is sufficient for one

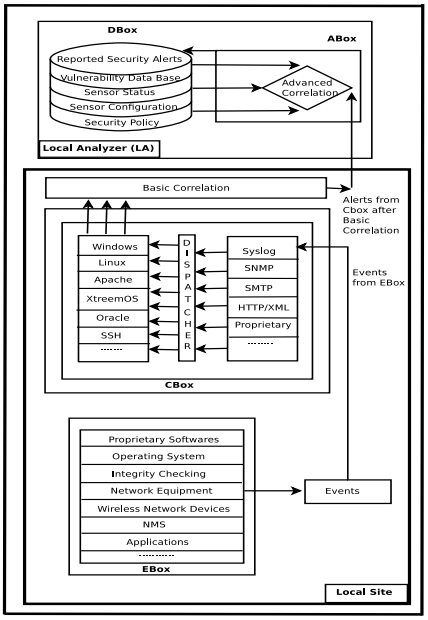


Figure 2: Intercommunication view of EBox, CBox and Local Analyzer

local site, but more than one CBox can be added depending on the number of active sensors and the amount of logs they generate. The Basic Correlation (BC) module has a defined time limit which holds the reported security alerts for one minute and correlates for detecting attacks. The Basic Correlation module forwards the correlated attack information to the Advanced Correlation (AC) module for detecting distributed attacks. The advanced correlation module collects logs from multiple CBoxes and further correlates for more sophisticated and distributed attacks. If an attack is detected, the ABox reports it to the administrator in real time and saves the security alert permanently in Local Intrusion Database (LIDB). The same reported alert will also be saved in the Global Intrusion Database (GIDB) as a backup of LIDB (see figure 4). LIDB is a database that contains all the core configurations related to the network devices, user configurations, security rules, and vulnerability database from Common Vulnerabilities Exposures (CVE) [26]. The mechanism for detecting distributed attacks using basic and advance correlation is discussed in detail in [25].

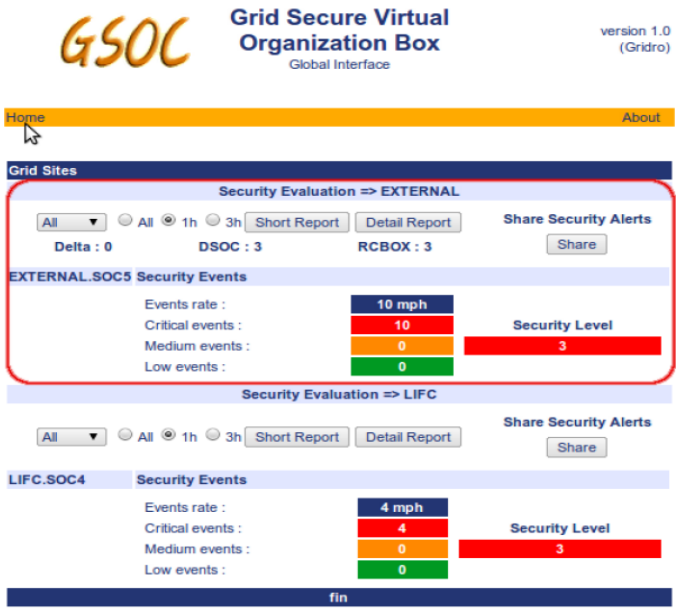


Figure 3: SVOBox Main Dashboard

3.2. GSOC Architecture Internal View

Figure 4 is the architectural internal view of each component of the GSOC. The reported alerts saved in the LIDB are also forwarded to the GIDB for security evaluation and to be shared with other ADs that compose the grid computing network. The GIDB consists of two parts. The upper part contains a replica of all configurations done within the LAs, reported security alerts from all the local sites of the AD and messages from all RCBoxes. The RCBoxes work like CBoxes except RCBoxes collect logs from the most important sensors in the AD. These sensors could be general security devices, proprietary softwares or customizable network monitoring systems. The purpose of collecting these logs is to double check the logs for network attacks. RCBoxes have been introduced in the GSOC design (i) to detect attacks that target security management devices (ii) when the attacker camouflages its attacks and (iii) when the attackers target GSOC components. The RCBoxes receive copies of the logs from the sensors and forward them to the GA. The GA correlates the received logs and forwards them to the GIDB. Thus, RCBox provides a way to compare the deviation (Δ) in the logs generated during normal operation of the network with the

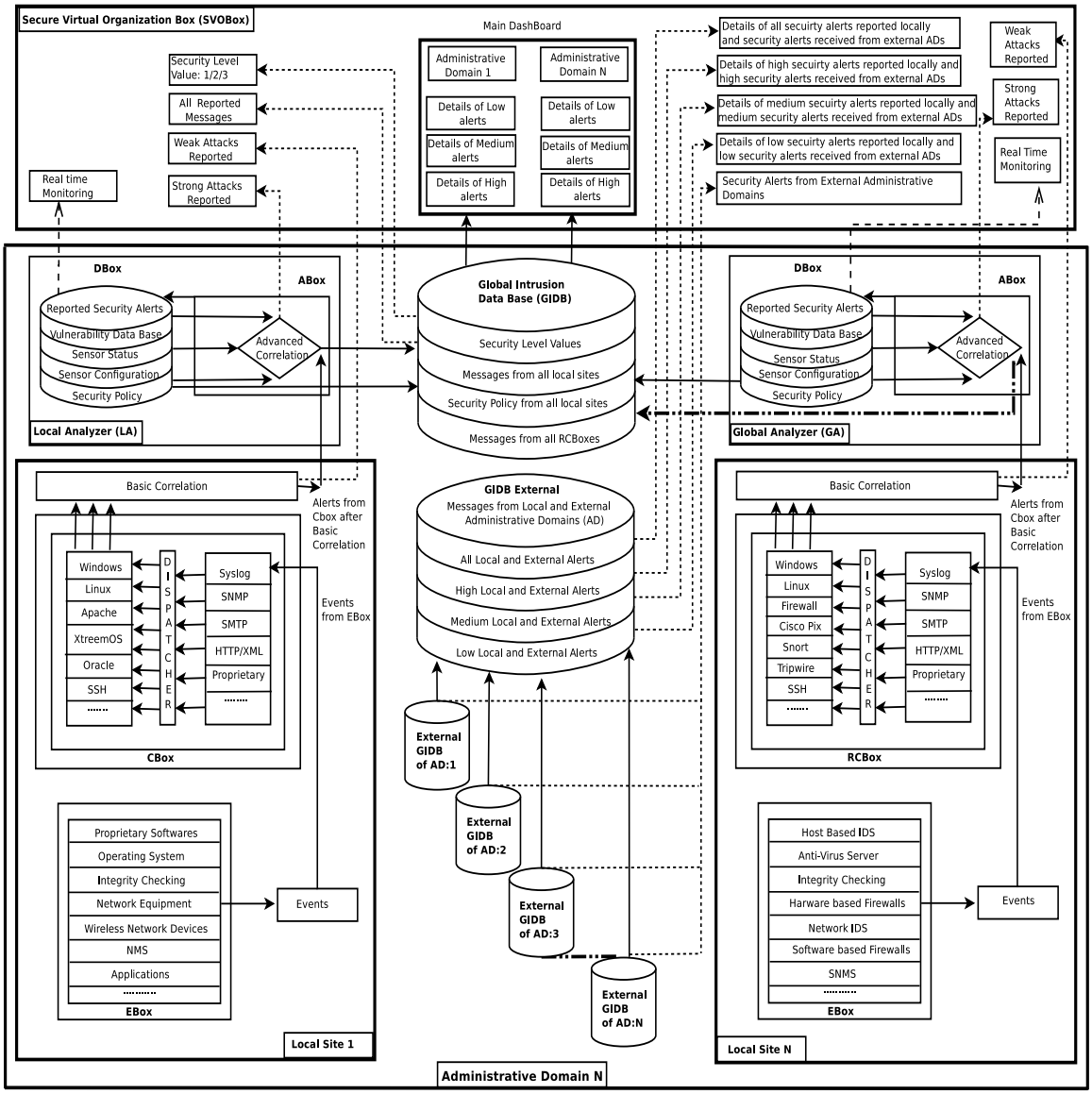


Figure 4: GSOC Internal Architectural View

abnormal behavior using GIDB. The deviation is calculated by comparing the message received in the GIDB from all local sites and the messages received from all RCBoxes. The deviation is directly proportional to the possibility of attacks.
Figure 3 shows the deviation (Δ), the messages received by the RCBoxes, the messages received from local sites, a short report, a detailed report, the security alert sharing option, and a security evaluation of two ADs. At the final stage the SVOBox evaluates the security level value for each AD. Security evaluation is discussed in detail in section 4.

The lower part of GIDB is called **External GIDB** and is responsible for sharing the reported security alerts with other ADs in a grid computing network. Security alert sharing can be very effective in blocking cross-domain attacks while keeping in view the composition of grid computing network which includes:

(i) Different ADs that consist of multi-local sites combined together to form a network.

(ii) The size of the network increases and decreases dynamically.

(iii) Nodes from one AD can collaborate with nodes from other ADs where different security policies are applied.

(iv) Both the administrator of the ADs whose nodes are communicating with each other do not know the nature of the attacks that are in progress at either side.

This raises the need for a solution that would provide the network administrators functionalities that can inform them of the nature of attacks that are under progress in any external ADs. One solution to this problem is to provide a way to share, between different ADs, their security alerts. But, sharing **all** security alerts of one entire network with another administrative is something that security policy should forbid. To address this issue GSOC provides a mechanism by which the network administrator of an AD can share specific security alerts with selected ADs depending on their security level of either low, medium, and high which rank the confidentiality of the alerts. The details of each category is discussed in detail in section 4. Figure 6 shows the overview of the reported security alert sharing mechanism between six administrative domains.

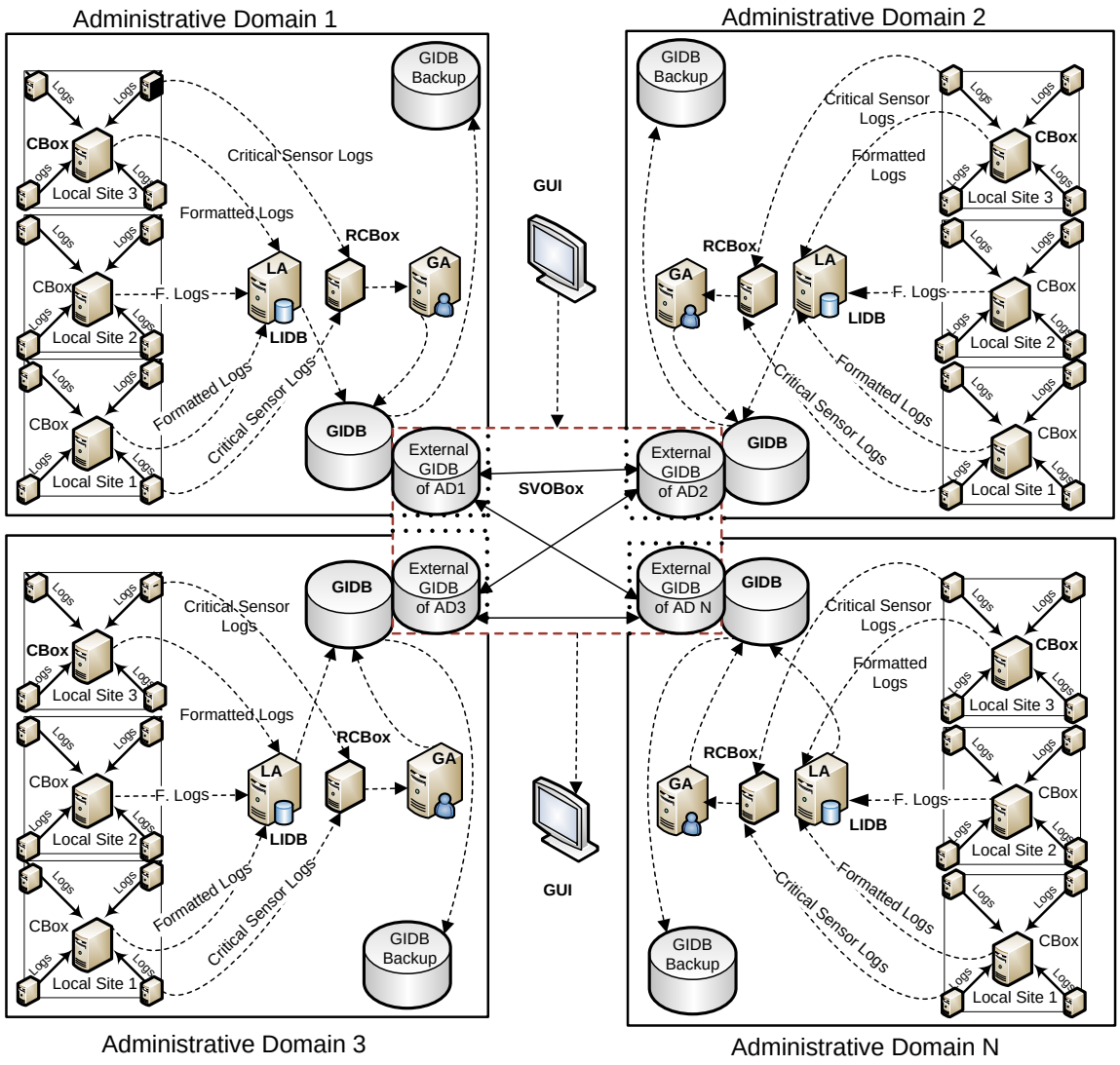


Figure 5: GSOC General Overview

SVOBox assigns security level values by manipulating the number of security alerts generated within the local sites of the AD. All the security alerts generated in different ADs of a grid network can be seen at the SVOBox main dashboard. The SVOBox dashboard access is granted to the network administrator of each AD. Only the ADs who are sharing their resources with each other are allowed to send and receive the security alerts between them (figure 3).

4. SECURITY EVALUATION OF ADMINISTRATIVE DOMAINS

Security evaluation of administrative domains that form a grid computing network is required in order to create trust between ADs. Security levels are a representation of the current security state of the AD. Evaluating the security of an AD which can be a multi-sites network is a complex task as it includes many heterogeneous devices. Security can be evaluated using multiple metrics. Some possibilities are:

(i) The skills of the IT security team that includes experience, certifications, trainings, and their availability.

(ii) The security devices and softwares used including (i.e., firewalls, intrusion detection and prevention systems (IDPS) and anti-virus softwares). Their configuration level includes the security rules and policies that must be updated on time.

(iii) Security contingency plans in case of severe attacks.

(iv) Time required to restore all the systems and services after shutdown in case of disasters.

(v) User awareness programs, for maintaining their system's security.

(vi) Reports of deep vulnerability scans, security scans, and pen tests must also be considered.

All the above mentioned aspects needs to be evaluated by a third party for non-biased evaluation results. We aim to provide an automated security evaluation of a dynamic network at a given time whereas security standard like ISO 27000 works on a progressive view of the security. we are using an automated security evaluation which takes into account dynamic network and its real-time constraints [27]. For evaluating security level values in GSOC, some equations written below have been applied to any AD which is a part

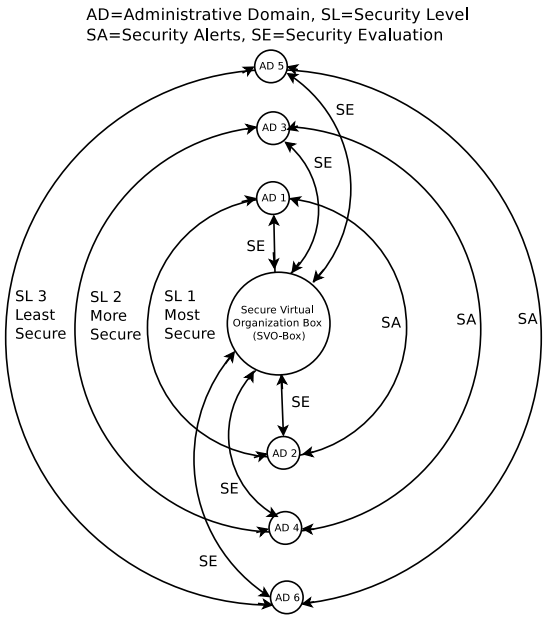


Figure 6: GSOC Security Alert Sharing Mechanism

of the grid computing network. These equations help GSOC to categorize the ADs by processing the number of low, medium and high alerts generated within their local sites. These levels are criticality levels that are assigned by to each alert by the network administrator of each AD. GSOC categorizes the ADs according to three security levels. Security level one is the highest security level while three is the lowest one (see figure 6).

Security evaluation of a network can also be done using tools like Nessus [28], OpenVAS [29] or Saint [30]. In GSOC the result of these three tools are also incorporated to give a better view to the administrator. Table 2 shows the number of security alerts detected during scan on 10 computers. The configuration of the computers are CPU 2.4 GHz and RAM 512 MB. Vulnerabilities are present in any software and they are reported at regular basis. There is a high possibility that many vulnerabilities can be reported if a machine contains lots of non-updated softwares. In our experiments, we used multiple machines with older and new release of updates.

LAV (Low Alert Value) is the number of low level alerts reported which are, for example, information like session opening, session closing, or services start/stop/restart. MAV (Medium Alert Value) is the number of medium

Table 2: **Security Evaluation Comparison of 10 Machines**

	OpenVas			Nessus			Saint		
M #	**LA**	**MA**	**HA**	**LA**	**MA**	**HA**	**LA**	**MA**	**HA**
M1	10	1	1	27	4	0	8	2	3
M2	10	1	1	27	4	0	11	2	0
M3	10	1	1	27	4	0	7	2	2
M4	28	4	1	96	16	0	14	2	3
M5	10	1	0	21	3	0	7	3	3
M6	10	1	1	26	4	0	8	2	1
M7	10	1	1	27	4	0	8	2	1
M8	10	1	1	26	4	0	8	2	0
M9	10	1	1	27	4	0	8	2	2
M10	7	1	0	30	2	0	7	1	1
Total	115	13	8	334	49	0	86	20	16

LA=Low Alerts, MA=Medium Alerts, HA=High Alerts, M#=Machine Number

alerts reported, and HAV (High Alert Value) is the number of high alerts reported in any AD. The behavior of the AD can be categorized according to three case :

Case-I: When an AD operates under normal circumstances, LAV is always greater than MAV, which is greater than HAV ($LAV > MAV > HAV$).

Case-II: There is a slight change in the normal behavior of an AD or in any one of its local sites. This happens when the inexperienced attackers try to launch basic attacks. Some examples might be, manual use of incorrect password attempts, port scans, and ICMP flooding. They use their personal machines without IP spoofing for launching these attacks, making these attacks easily detectable.

Case-III: There is a major change in the normal behavior of an AD or in any one of its local sites. This case occurs when the experienced attackers use multiple machines for launching distributed attacks. They use automated tools and spoof their IPs. The duration of the attacks last for a very long period of time and they mix their attacks with normal behavior to camouflage their operations. These attacks are difficult to detect and very destructive

in nature. Some of the examples of these attacks are the use of brute force attacks using automated tools such as THC Hydra [2] & Guess Who [3], DoS & DDoS attacks using Slowloris [31], and UDP & TCP flooding by changing the maximum transmission unit (MTU) of the packets.

NOTE: The standard policy must be adopted by all members of the grid computing network for assigning the critical values to the attacks in order to have a homogeneous reporting systems.

Formalization of Security Evaluation
LA = Low Alerts. MA = Medium Alerts. HA = High Alerts. LAV = Low Alerts Value. MAV = Medium Alert Value. HAV = High Alert Value. SL = Security Level. GN = Grid Network. LS = Local Site. LSA = Local Sites Alerts. t = time at which the alerts detected. L = Low, M = Medium and H = High.

Let GN be a grid computing network:

$$GN = \{AD_1, AD_2, ...AD_m\}$$

with

$$AD_{(i)} = \{LS_{(i)}1, LS_{(i)}2, ...LS_{(i)}n_i\}$$

where n_i is the number of local sites of the administrative domain, and m is the number of administrative domains in GN. Now LAV, MAV and HAV at time "t" can be determined by:

$$LAV \longmapsto LA_{(ADi)}(t) = \sum_{j=1}^{n_i} LSA_L(t)$$

LAV is the number of total low alerts reported within all local sites of an AD.

$$MAV \longmapsto MA_{(ADi)}(t) = \sum_{j=1}^{n_i} LSA_M(t)$$

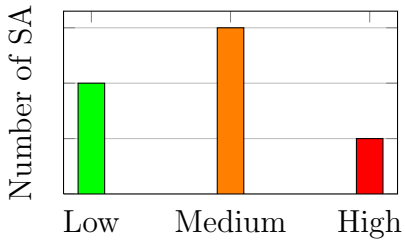
MAV is the number of total low alerts reported within all local sites of an AD.

$$HAV \longmapsto HA_{(ADi)}(t) = \sum_{j=1}^{n_i} LSA_H(t)$$

HAV is the number of total low alerts reported within all local sites of an AD.

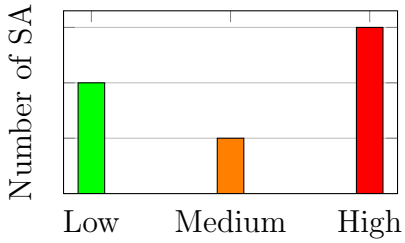
Now the AD can be set to SL1, SL2 or SL3, if any of the equations from 1 to 6 matches with the LAV, MAV, and HAV conditions.
Equation 1 shows that the AD has medium security alerts greater than low and high, whereas low security alerts; are greater than high security alerts, therefore it should be placed in SL2 (see graph).

$$\boxed{(LAV_{(AD)} < MAV_{(AD)}\ and\ LAV_{(AD)} > HAV_{(AD)})\ then\ SL = 2} \quad (1)$$



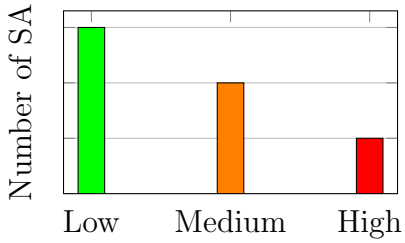
Equation 2 shows that the AD has high security alerts greater than low and medium, whereas low security alerts are greater than medium security alerts; therefore it should be placed in SL3 (see graph).

$$\boxed{elseif(LAV_{(AD)} > MAV_{(AD)}\ and\ LAV_{(AD)} < HAV_{(AD)})\ then\ SL = 3} \quad (2)$$



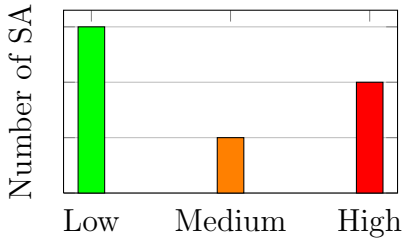
Equation 3 shows that the AD has low security alerts greater than high and medium, whereas medium security alerts are greater than high security alerts; therefore it should be placed in SL1 (see graph).

$$\boxed{elseif(LAV_{(AD)} > MAV_{(AD)}\ and\ MAV_{(AD)} > HAV_{(AD)})\ then\ SL = 1} \quad (3)$$



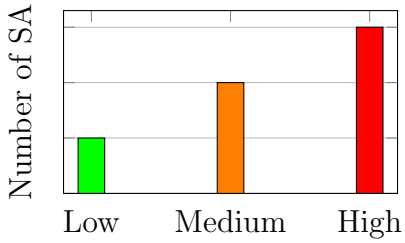
Equation 4 shows that the AD has low security alerts greater than high and medium, whereas high security alerts are greater than medium security alerts; therefore it should be placed in SL2 (see graph).

$$\boxed{elseif(MAV_{(AD)} < LAV_{(AD)}\ and\ HAV_{(AD)} < LAV_{(AD)})\ then\ SL = 2} \quad (4)$$



Equation 5 shows that the AD has high security alerts greater than low and medium, whereas medium security alerts are greater than low security alerts; therefore it should be placed in SL3 (see graph).

$$\boxed{elseif(MAV_{(AD)} > LAV_{(AD)}\ and\ MAV_{(AD)} < HAV_{(AD)})\ then\ SL = 3} \quad (5)$$



Equation 6 shows that the AD has medium security alerts greater than low and high, whereas high security alerts are greater than low security alerts; therefore it should be placed in SL3 (see graph).

$$\boxed{elseif(MAV_{(AD)} > LAV_{(AD)}\ and\ MAV_{(AD)} > HAV_{(AD)})\ then\ SL = 3} \quad (6)$$

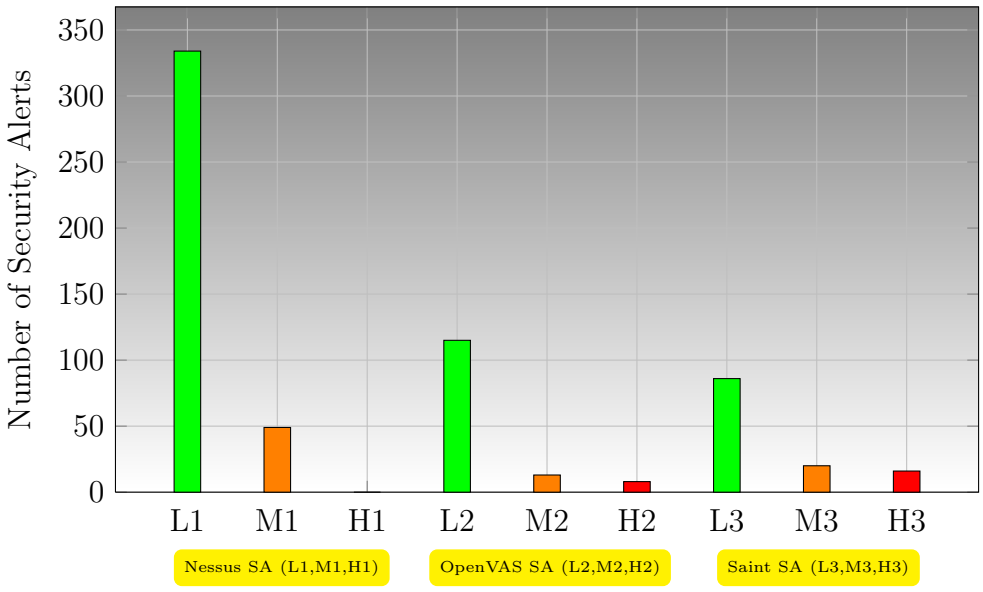


Figure 7: Security Alert Statistics of 10 Machines using Nessus, OpenVAS and Saint

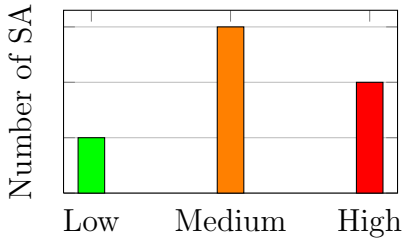


Figure 7 is the graphical representation of the data of 10 machines that shows that in normal circumstances the low alerts are always greater than medium and high alerts. These results are taken by the scan from Nessus, OpenVAS and Saint, and validate the equations used for security evaluation in GSOC.

5. EXPERIMENTS AND RESULTS

This section compares the behavior of two types of security management systems. The first one is developed for traditional computer network, but could be deployed in grid computing networks; the second one is developed for grid computing networks. The Distributed Security Operation Center

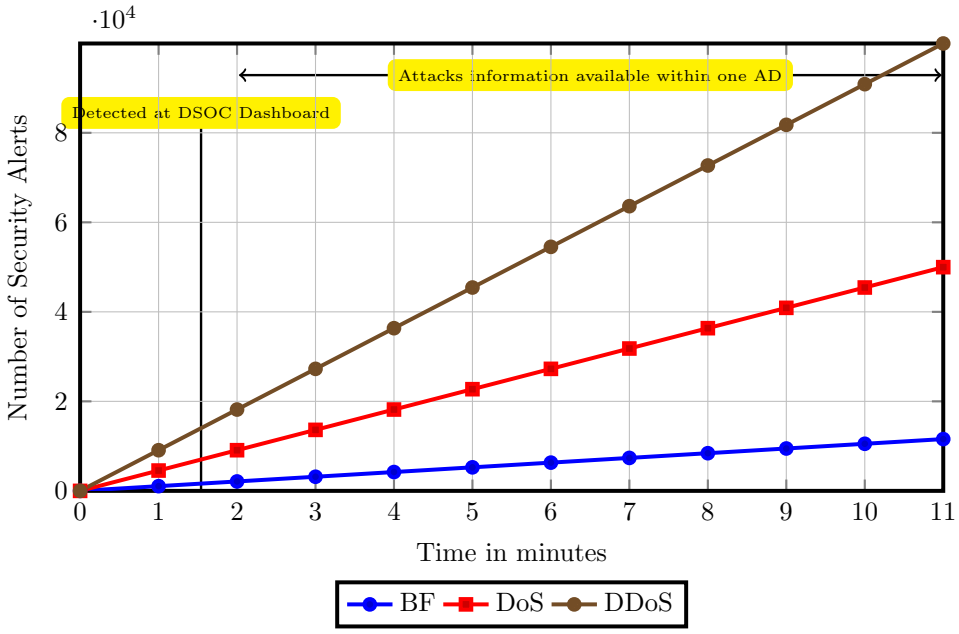


Figure 8: Detection rate of BF, DoS and DDoS in Distributed Security Operation Center (DSOC)

(DSOC), which while developed for traditional computer networks has been used for executing different tests is classified in figure 1 under the category "Security solutions for traditional networks deployable in grid computing networks." The DSOC will be used for representing other security solutions that exist in a similar category. Graphs 8 and 9 show the security alert rate in minutes. The graphs shows three attack details, namely those of Brute Force attacks (BF), Denial of Service attacks (DoS), and Distributed Denial of Service attacks (DDoS) launched on DSOC and on GSOC using multiple sites of the Grid'5000 (G5K) network. The details of the network can be seen at [32].

5.1. Attack Scenario-I

Figure 10 consists of two parts. The upper part represents a simplified view of G5K network with CBox running at the Rennes site. The LA+ABox, LIDB, GA+GIDB are running at the Nancy site. The approved users are allowed access to these sites where they can reserve many nodes and perform their experiments. These users are also allowed to reserve any number of machines between nine other sites of the G5K.

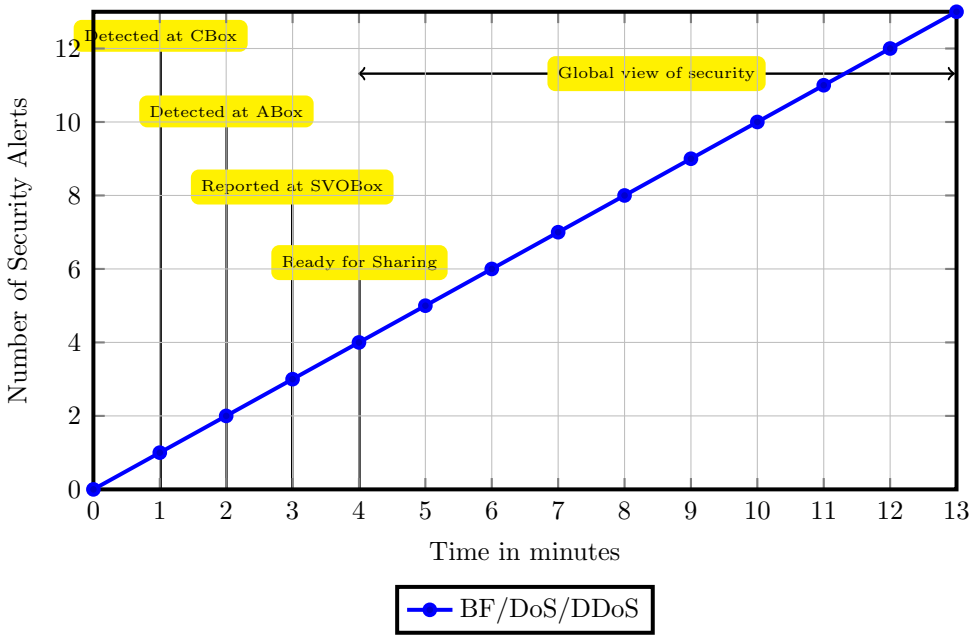


Figure 9: Detection rate of BF, DoS and DDoS in Grid Security Operation Center (GSOC)

The lower part is a simplified view of our lab network where two users from Machine 1 and 2 via ssh connection ① & ② are allowed to connect into the G5K network. Attackers 1 & 2 try to get access to machines 1 and 2 by launching brute force attacks using a dictionary of passwords that contains 8048 passwords. Attacker 2 was not successful on Machine 1 due to a strong password. Attacker 1 was successful and cracked the password of Machine 2 after 10 minutes which is found at the 5000th location of the password file③. Attacker 1 using machine 2 is a threat within local and external networks which are connected together. Attacker 1 can perform malicious activities in G5K since the connection originated from the approved user machine. For the G5K network, Machine 1 was a trusted machine but is now compromised; ④ shows that the G5K network is accessible by Attacker 1. Attacker 1 can further launch more brute force attacks on other machines of the G5K. If successful, the results are very destructive.

5.2. Attack Scenario-II

Usually, an experienced attacker uses a combination of multiple attacks to hide their activities. The easiest scenario is to first launch a DoS attack from

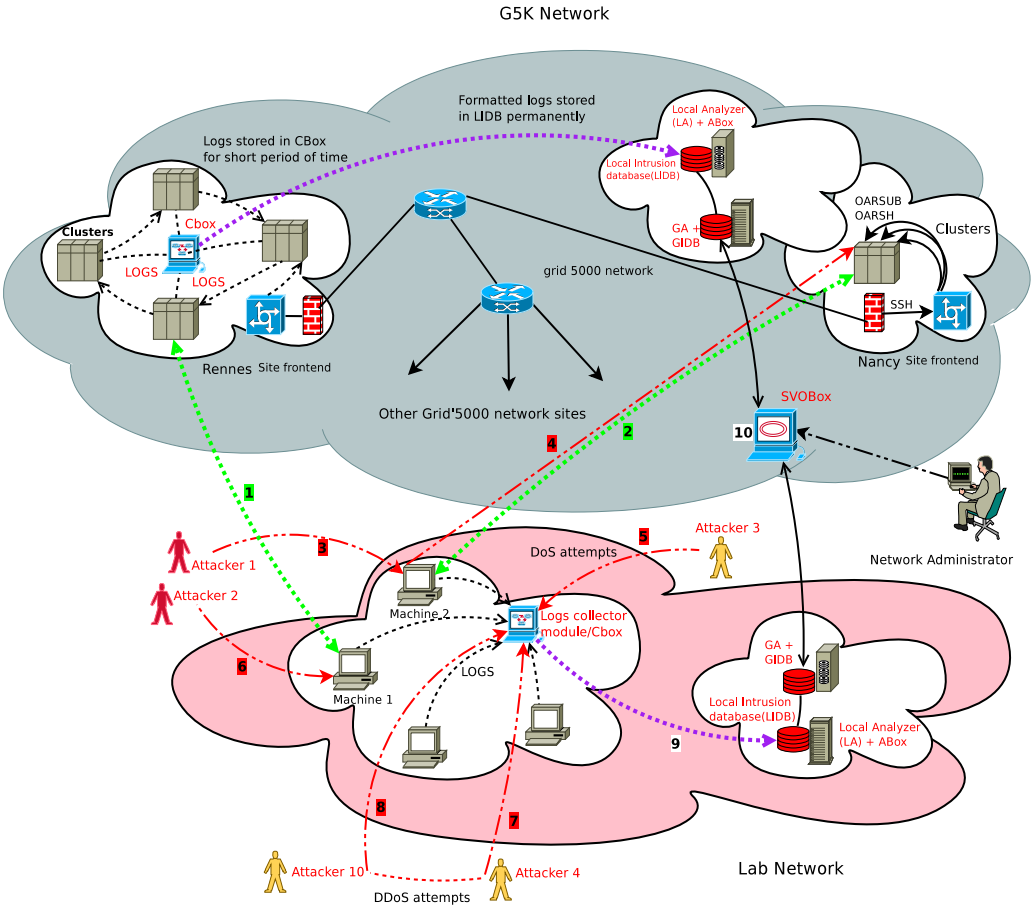


Figure 10: Stopping propagation of cross-domain attacks between our lab and G5K network

Attacker 3 that generates the alerts of DoS ⑤. These alerts are generated deliberately to attract the attention of the network administrator and fill the GUI of the security management system. After some time Attacker 2 from the other machine starts launching another attempt of brute force attacks ⑥ to crack the password of Machine 1. These attacks last for short periods of time and are restarted after some time.

5.3. Attack Scenario-III

A more complex scenario is to launch the DDoS from multiple machines (Attacker 4 to Attacker 6) by spoofing IP addresses ⑦ & ⑧. These attackers generate several alerts and because of the IP spoofing need more time from the administrator to detect the actual source of the attacks. These attacks cover two objectives: It overloads the network and its components so the legitimate users cannot access it and allows them to destabilize the security management systems. In this way, the malicious activities are not easily detectable and if they are detected, they will be reported very late to the administrator due to the high number of security alerts processing time.

By deploying GSOC between G5K and our lab network, attack types I, II & III can be blocked at very early stage. The CBox which is running in our network collects all unsuccessful authentication failures attempts and sends them to the LA ⑨. The LA correlates all the logs, generates a brute force attack attempts, and saves it in LIDB. The sharing mechanism of GSOC allows the lab network to share this information with the G5K network. The administrator of the G5K network has access to the brute force attempt alarm in our lab which includes the IP address, user ID, start time of attack, end time of attack, and total number of fail attempts ⑩. This information helps the network administrator of G5K to stop the access of that user. In this way an attack which is propagated from one administrative domain to another can be blocked.

In figure 8 the DSOC detects the attacks between 1 or 2 minutes and reports them at the dashboard. The DSOC generates an alarm for almost every attempt. These alarms utilize network bandwidth in case of a multi-site network, and they use a reasonable amount of disk space if the attacks continue for long periods of time. The reported security alarms are only available within the premises of one AD. This limitation does not suit grid networks as there are attacks that use computer worms which expands by themselves. These attacks could therefore expand to other members of a grid network. A mechanism has therefore been adopted in GSOC for sharing

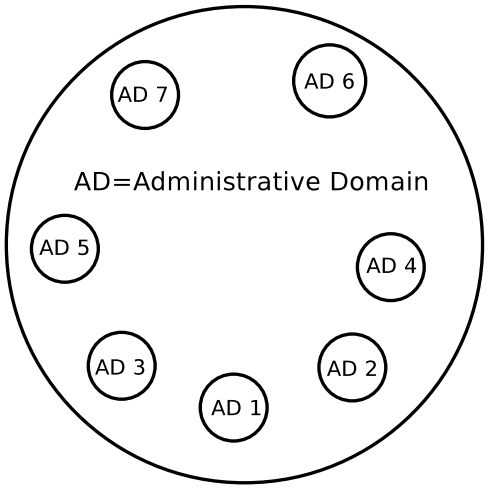


Figure 11: No Mechanism for Security Alert Sharing in Grid Computing Network Scenario

reported security alerts between multiple ADs to protect other members in a grid network for possible cross-domain attacks. See figure 11 where there is no security alert sharing mechanism. This scenario can lead to propagate some serious network attacks to other members of the grid. In figure 12 the security mechanism exists but it is not intelligent because ADs are sharing security alerts randomly. This sharing of information cannot be result oriented as it uses more network bandwidth and exposes internal security information to insecure ADs. Keeping these issues in mind, an efficient approach is to share the security alerts after classifying the ADs. See figure 6 for a depiction of security evaluation through the assignment of sharing mechanisms into three categories SL1 as most secure, SL2 as more secure, and SL3 as least secure. This classification gives a global view of security within a grid network to its members.

In figure 9 the GSOC detects the attack within one minute on the CBox. By the second minute they are detected on the ABox, which correlates the alerts coming from multiple local sites and discards false positives. By the third minute the details of the attacks are available on the SVOBox. By the fourth minute all alerts are ready for sharing with other ADs in a grid computing network. This can help blocking cross-domain attacks. It utilizes less bandwidth and disk space and gives a global view of security for the entire grid network.

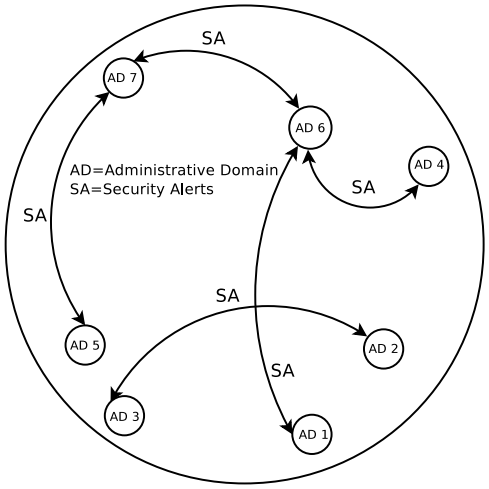


Figure 12: Unintelligent Mechanism for Security Alert Sharing in Grid Computing Network Scenario

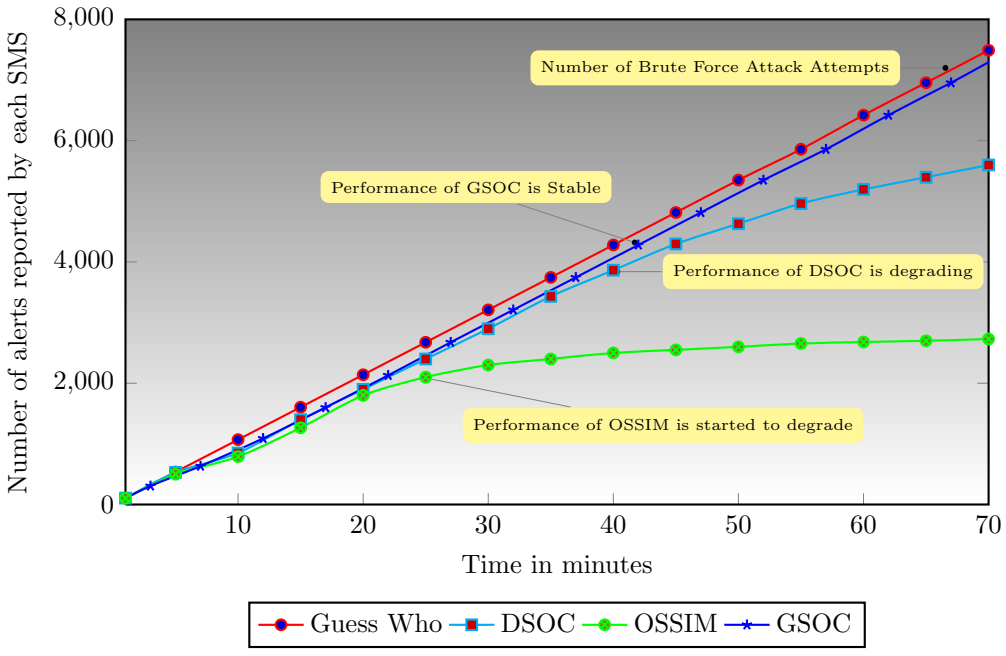


Figure 13: Stability of different Security Management Systems

6. DISCUSSION

Due to the nature of grid computing networks, a security management system must comply to some basic factors. According to our research the most important are scalability, fault-tolerance, security alerts correlation, security evaluation, and security alert sharing. GSOC covers all these factors as it has scalability due to its modular design. It can handle networks that are growing dynamically. RCBox provides fault-tolerance capability in case if any of the CBox fails or comes under attack. GSOC has two step correlation basic and advance which help to keep it stable especially when the grid network is under DDoS attacks. GSOC has dynamic and static security evaluation which informs the member of the grid about the members that are vulnerable to the attacks. This helps to share their resources with them by applying more strict security policies. SVOBox provides security alerts sharing mechanism which is the most important factor in blocking cross-domain attacks. OSSIM and GSOC are suitable to be deployed in grid computing network to manage its security as shown in Table 1. Subsection 6.1 shows a small test about the performance of these systems. OSSIM [33] is a product of Alien Vault Professional Corporation. It is an open source freely available Security Information and Event Management (SIEM) system but some advance reporting capabilities are not freely available. It is a framework for the management of the security infrastructure of the large organizations.

6.1. Stability Comparison of Security Management Systems

Figure 13 is the graphical view which shows the comparison of different security management systems (SMS). It shows the degradation in performance when the high intensity of attack continues for long period of time on the SMS. For comparing the performance of each SMS one round of BF attack was perform on a machine using a list of passwords. Guess Who [3] performed more than 8000 passwords attempts on one victim machine. The red line in figure 13 shows the number of attempts made by the attacker on the victim machine. To detect this attack three SMS namely GSOC, DSOC and OSSIM are placed in parallel. The detection rate of GSOC remains stable throughout the attack. The detection rate of DSOC remains stable until 35 minutes but after that it starts degrading its performance. The detection rate of OSSIM remains stable until 20 minutes but after that it also starts degrading its performance. Both the DSOC and OSSIM detects the attacks but when the attack continues for long period of time there performance

become bad to worse. This performance degradation is very crucial if the attacker gets success in its attacks. Due to this reason the alerts are reported with the delay and the delay continue to increase as shown in the graph. In this case even the DSOC and OSSIM will detect attack after a certain delay but this delay give a fair chance to the attacker to do some harmful activities successfully. Whereas in the case of GSOC it continue detecting the attacks with a negligible delay.

7. CONCLUSION AND FUTURE WORK

Grid computing networks are complex environments to protect as they raise multiple challenges, one of them being the heterogeneous structure of a grid network which can be composed of different administrative domains. This heterogeneity lowers the possibility of alert sharing and therefore decreases the protection of the network when dealing with cross-domain attacks. In this paper, we have proposed GSOC which fulfills all the prerequisites for becoming a prototype security solution for grid computing networks. The distributed and modular architecture of GSOC allows it to scale up to the size of the grid computing network. The experiments have shown a network administrator of any AD can share its security alerts at any time with others. In case of a severe distributed attack GSOC can give a global view of the network security after 4 minutes while other tools have failed to do so. The classification of the ADs in security levels using security evaluation creates a trust between the members of the grid network. Alert sharing mechanisms can still be improved. Depending on the security policy, on the criticality level of the alerts and on the security level of the AD, a customizable anonymity of alerts based on [34, 35] could be used in order to be able to share even the most critical alerts and therefore improving the correlation.

In cloud computing networks the most recent issues are discussed by Balduzzi et al. [36]. They performed vulnerability tests on 5000 virtual machine images available in four different data centers of Amazon [37] and reported several security issues in public virtual images. Bugiel et al. [38] also raised the similar issues but they performed experiments on 1255 Amazon images and the scope of their experiments was limited in covering security issues. Garfinkel and Rosenblum [39] highlighted the use of third party virtual images and their security issues. Glott et al. [40] discussed the security issues that occurs when the virtual images are shared within multiple users in cloud infrastructure. Bleikertz at al. [41] used graph theory techniques to deploy

secure virtual machine images in Amazon EC2 infrastructure. The main focus of all the researchers is to emphasis that there exists some serious security threats in cloud computing infrastructures. GSOC can be deployed in cloud computing infrastructure after certain modifications and can address these issues up to certain extend. New boxes should be introduced at each service, that means one box for infrastructure, one for platform and one for software. These boxes must be programmed to handle the specific security issues occurred at each service level and verify newly added and modified images by the cloud users. If found a vulnerability in any image, they must block that image for other users. These boxes must works separately and report to the LA, but if needed can also collaborate to detect the attacks which are launched using all the three service levels. For every service there can be a separate LA. All the LAs at each service level must report to the GA which will handle the security of the entire cloud. Multiple SVOBoxes can be used if the cloud network is composed of hybrid or multi-public clouds. The manager of all the boxes will be the Cloud Box (CLBox).

References

[1] W. R. Cheswick, S. M. Bellovin, A. D. Rubin, Firewalls and Internet Security; Repelling the Wily Hacker, Addison-Wesley, Reading, MA, second edition, 2003.

[2] V. Hauser, The hacker's choice, a very fast network logon cracker which support many different services, Available from: http://freeworld.thc.org/, 2010.

[3] Guess who is a password brute force utility for attacking secure shell version 2 accounts, Available from: http://www.vulnerabilityassessment.co.uk/guesswho.htm, 2010.

[4] K. F. Bart Jacob, Michael Brown, N. Trivedi, Introduction to Grid Computing, IBM Corp., 2005.

[5] S. Tuecke, V. Welch, D. Engert, L. Pearlman, M. Thompson, Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile, RFC 3820 (Proposed Standard), 2004.

[6] M. Cremonini, S. D. C. di Vimercati, E. Damiani, P. Samarati, An xml-based approach to combine firewalls and web services security specifications, in: Proceedings of the 2003 ACM workshop on XML security, XMLSEC '03, ACM, New York, NY, USA, 2003, pp. 69–78.

[7] A. Chakrabarti, Grid Computing Security, Springer, 2007.

[8] Globus: Grid security infrastructure (gsi), http://www-unix.globus.org/toolkit/docs/3.2/security.html, 2010.

[9] Public-key infrastructure (pki), Accessed from: http://datatracker.ietf.org/wg/pkix/charter/, 2011.

[10] E. Cody, R. Sharman, H. R. Rao, S. J. Upadhyaya, Security in grid computing: A review and synthesis, Decision Support Systems 44 (2008) 749–764.

[11] U. Schwiegelshohn, R. M. Badia, M. Bubak, M. Danelutto, S. Dustdar, F. Gagliardi, A. Geiger, L. Hluchý, D. Kranzlmüller, E. Laure, T. Priol, A. Reinefeld, M. M. Resch, A. Reuter, O. Rienhoff, T. Rüter, P. M. A. Sloot, D. Talia, K. Ullmann, R. Yahyapour, Perspectives on grid computing, Future Generation Comp. Syst. 26 (2010) 1104–1115.

[12] M. Coppola, Y. Jégou, B. Matthews, C. Morin, L. P. Prieto, O. D. Sánchez, E. Y. Yang, H. Yu, Virtual organization support within a grid-wide operating system, IEEE Internet Computing 12 (2008) 20–28.

[13] J. Bourgeois, S. R. Hassan, Managing security of grid architecture with a grid security operation center., in: SECRYPT'09, Int. Conf. on Security and Cryptography, Milan, Italy, INSTICC Press, 2009, pp. 403–408.

[14] S. Kenny, B. Coghlan, Towards a grid-wide intrusion detection system, in: Advances in Grid Computing - EGC 2005, volume 3470 of *Lecture Notes in Computer Science*, Springer Berlin / Heidelberg, 2005, pp. 275–284.

[15] Snort network intrusion prevention and detection system (ids/ips), Available from: http://www.snort.org/, 2010.

[16] F. Y. Leu, J. C. Lin, M. C. Li, C. T. Yang, P. C. Shih, Integrating grid with intrusion detection, International Conference on Advanced Information Networking and Applications, Volume 1 (2005) 304–309.

[17] F. Y. Leu, J. C. Lin, M. C. Li, C. T. Yang, A performance-based grid intrusion detection system, in: COMPSAC '05: Proceedings of the 29th Annual International Computer Software and Applications Conference (COMPSAC'05) Volume 1, IEEE Computer Society, Washington, DC, USA, 2005, pp. 525–530.

[18] F. Y. Leu, M. C. Li, J. C. Lin, Intrusion detection based on grid, in: Proceedings of the International Multi-Conference on Computing in the Global Information Technology, IEEE Computer Society, Washington, DC, USA, 2006, pp. 62–67.

[19] Prelude is a universal "security information event management" (siem) system, www.prelude-technologies.com/en/development/documentation/index.html, 2012.

[20] Y. Chu, J. Li, Y. Yang, The architecture of the large-scale distributed intrusion detection system., in: PDCAT'05, pp. 130–133.

[21] P. F. Silva, C. B. Westphall, C. M. Westphall, M. D. Assunção, Composition of a dids by integrating heterogeneous idss on grids, in: Proceedings of the 4th international workshop on Middleware for grid computing, MCG '06, ACM, New York, NY, USA, 2006, pp. 12–.

[22] A. K. Ganame, J. Bourgeois, R. Bidou, F. Spies, A global security architecture for intrusion detection on computer networks, Computers & Security 27 (2008) 30–47.

[23] S. Northcutt, J. Novak, Network Intrusion Detection, ISBN: 0-73571-265-4, New Riders, third edition edition, 2002. September.

[24] J. Bourgeois, R. Bidou, F. Spies, Towards a global security architecture for intrusion detection and reaction management, in: K. Chae, M. Yung (Eds.), Proc. of the 4th Int. Ws. on Information Security Applications, WISA 2003, volume 2908 of *LNCS*, Jeju, Corea, pp. 129–142.

[25] S. R. Hassan, J. Pazardzievska, J. Bourgeois, Minimization of security alerts under denial of service attacks in grid computing networks, in: International Conference on Grid Computing and Applications (GCA) at Las Vegas, USA. 2011.

[26] Common vulnerabilities and exposures is a dictionary of publicly known information security vulnerabilities and exposures, Access from: http://cve.mitre.org/, 2010.

[27] G. A. Karim, J. Bourgeois, 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 (2008) 1 – 8.

[28] Security scanner for oracle and various flavors of unix, Available from : www.nessus.org/, 2010.

[29] The open vulnerability assessment system (openvas), Available from : www.openvas.org/, 2010.

[30] Vulnerability management, assessment, penetration testing (saint), Available from : www.saintcorporation.com/, 2010.

[31] RSnake, J. Kinsella, Slowloris http denail of service, Available from: http://ha.ckers.org/slowloris/, 2010.

[32] Grid'5000 is a scientific instrument for the study of large scale parallel and distributed systems., Access from: https://www.grid5000.fr/mediawiki/index.php/Grid5000:Home, 2010.

[33] Open source security information and event management (ossim), Access from:http://alienvault.com/resources/documentation/technical-documentation, 2011.

[34] P. Jurczyk, L. Xiong, S. Goryczka, Dobjects+: Enabling privacy-preserving data federation services, in: 28th IEEE International Conference on Data Engineering (ICDE).2012.

[35] Y. Xiao, J. Gardner, L. Xiong, Dpcube: Releasing differentially private data cubes for health information, in: 28th IEEE International Conference on Data Engineering (ICDE).2012.

[36] M. Balduzzi, J. Zaddach, D. Balzarotti, E. Kirda, S. Loureiro, A security analysis of amazon's elastic compute cloud service, in: Proceedings of the 27th Annual ACM Symposium on Applied Computing, SAC '12, ACM, New York, NY, USA, 2012, pp. 1427–1434.

[37] Amazon elastic compute cloud (amazon ec2), Available at : http://aws.amazon.com/ec2/, 2012.

[38] S. Bugiel, S. Nürnberger, T. Pöppelmann, A.-R. Sadeghi, T. Schneider, Amazonia: when elasticity snaps back, in: Proceedings of the 18th ACM conference on Computer and communications security, CCS '11, ACM, New York, NY, USA, 2011, pp. 389–400.

[39] T. Garfinkel, M. Rosenblum, When virtual is harder than real: security challenges in virtual machine based computing environments, in: Proceedings of the 10th conference on Hot Topics in Operating Systems - Volume 10, HOTOS'05, USENIX Association, Berkeley, CA, USA, 2005.

[40] R. Glott, E. Husmann, A.-R. Sadeghi, M. Schunter, Trustworthy clouds underpinning the future internet, in: IEEE Signal Process. Lett.'11, pp. 209–222.

[41] S. Bleikertz, M. Schunter, C. W. Probst, D. Pendarakis, K. Eriksson, Security audits of multi-tier virtual infrastructures in public infrastructure clouds, in: Proceedings of the 2010 ACM workshop on Cloud computing security workshop, CCSW '10, ACM, New York, NY, USA, 2010, pp. 93–102.