Future Generation Computer Systems 29 (2013) 536–547

Contents lists available at SciVerse ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Protecting grids from cross-domain attacks using security alert sharing mechanisms[☆]

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

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

ARTICLE INFO

Article history:
Received 6 February 2012
Received in revised form
28 June 2012
Accepted 14 July 2012
Available online 27 July 2012

Keywords:
Security management of grid computing networks
Security alert sharing
Security level assessment
Blocking cross domain attacks
Security evaluation in grid computing networks

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 the Grid Security Operation Center (GSOC), which facilitates 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 alert sharing scheme. Alert sharing can then be tuned in order to meet local security policy rules.

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 break them [1–3]. However usage of a manually set password does 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 maintain 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 organization's network. The attackers also exploit 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 action on the hosts and the 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 the 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 another organization's network which is part of that grid network.

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

[*] Corresponding author. Tel.: +33 381 994787; fax: +33 381 994791.
E-mail addresses: raheel.hassan@gmail.com, raheel.hasan@univ-fcomte.fr (R.H. Syed), maxime.syrame@edu.univ-fcomte.fr (M. Syrame), julien.bourgeois@femto-st.fr (J. Bourgeois).
URL: http://lifc.univ-fcomte.fr/~bourgeoi (J. Bourgeois).

0167-739X/$ – see front matter © 2012 Elsevier B.V. All rights reserved.
doi:10.1016/j.future.2012.07.002

1.3. Proposed suggestions for improving the security of grid computing

Keep in mind that 100% 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 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 to 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

Fig. 1 shows the classification of different types of monitoring and security management tools. Kenny and Coghlan [14] proposed *SANTA-G* (Grid-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 cannot 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 lowers 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 detect cross-domain attacks.

Fang-Yie Leu et al. propose three versions of an intrusion detection system dedicated to grid networks: GIDS (Grid Intrusion Detection System), PGIDS (Performance GIDS), and FGIDS (Fault-tolerant GIDS) [16–18]. 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 the 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 match 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 propose 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. 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 the *Large-Scale Distributed Intrusion Detection System (LDIDS)* proposed by Chu 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 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. DIDoS does not provide a mechanism for sharing alerts between the different administrative domains.

The *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). Fig. 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.