Design and Evaluation of a Grid Computing Based Architecture for Integrating Heterogeneous IDSs

Paulo F. Silva, Carlos B. Westphall, Carla M. Westphall
Network and Management Laboratory
Federal University of Santa Catarina, Florianópolis, Brazil
E-mail: {paulo, westphal, carla}@lrg.ufsc.br

Marcos Dias de Assunção
Grid Computing and Distributed Systems Laboratory
Department of Computer Science and Software Engineering
The University of Melbourne, Victoria, Australia
E-mail: marcosd@csse.unimelb.edu.au

Abstract—Intrusion Detection Systems (IDSs) have been substantially improved in recent past. However, network attacks have become more sophisticated and increasingly complex: many of current attacks are coordinated and originated in multiple networks. To detect these attacks, IDSs need to obtain information on network events from multiple networks or administrative domains. This work demonstrates that a Distributed IDS (DIDS) can be composed of existing IDSs, improving the detection of misuses in a multiple network environment. We use a Grid middleware for creating a service-based intrusion detection Grid. We demonstrate through experimental results that the proposed DIDS allows the integration of heterogeneous existing IDSs and improves the detection of attacks by exploring the synergy between existing IDSs.

Index Terms—Distributed Intrusion Detection Systems, Grid Services, Globus, IDS Composition.

I. INTRODUCTION

Distributed Intrusion Detection Systems (DIDSs) started to emerge in early 90s due to the need to correlate information from multiple network domains in order to detect distributed attacks [1]. Since then, research on DIDSs has received much interest, mainly because centralised and monolithic Intrusion Detection Systems (IDSs) are not able to provide enough information to prevent attacks that are coordinated and originated in multiple networks. The research community and industry have proposed varying solutions for integrating heterogeneous IDSs [2]–[5]. The Intrusion Detection Working Group IDWG highlights several reasons and benefits of integrating IDSs [6].

Although a DIDS can allow the detection of distributed attacks, it requires a high degree of coordination among its components and can be complex and difficult to maintain. Moreover, the use of multiple tools for intrusion detection or the integration of existing IDSs are neither straightforward nor easy tasks; they demand the design and implementation of protocols for communication, data transfer, among others. In this case, Grid computing is appealing as it enables the development of distributed applications and coordination in a distributed environment [7].

Grid computing aims to enable coordinated resource sharing within dynamic groups of individuals and/or physical organisations. Grid middleware enables for secure access, management and allocation of remote resources; and provides resource information services and protocols and mechanisms for data transfer [8]. Grid systems, driven by Service Oriented Architectures (SOAs), have been structured as networks of interoperating services that communicate with one another via standard interfaces [9]. In this scenario, resources and existing applications can be encapsulated and provided as services to end users. We envision that IDSs can also be encapsulated and delivered as services to users.

In our previous work, we proposed an architecture based on Grid computing technology for the composition of a DIDS, through the encapsulation of existing IDSs as Grid services [10]. We have demonstrated the usefulness of this integration through simulation using GridSim Toolkit [11]. Here, we describe the implementation of our architecture using Globus Toolkit 4.0.1 [12], complying with the WSRF specifications [9]. The proposed system, termed Distributed Intrusion Detection System on Grid (DIDSoG) enables heterogeneous IDSs to work together in a cooperative way. We design a common interface to integrate IDSs to DIDSoG. Each IDS is viewed as a resource accessed through WSRF interfaces. DIDSoG uses WSRF compliant services offered by Globus including: communication (i.e. XML and SOAP), Grid Security Infrastructure (GSI) and Monitoring and Discovery Service (WS-MDS).

The rest of this paper is organised as follows. Section II presents related work. Section III describes the proposed system. The development of DIDSoG is discussed in Section IV. We present and discuss experimental results in Section V. Section VI concludes the paper and presents the future work.

II. RELATED WORK

Sterne et al. present a hierarchical architecture for a DIDS in which information is collected, aggregated, correlated and analysed as it is sent up in the hierarchy [13]. Components in the same level of the hierarchy cooperate with one another. Similarly, the integration proposed by DIDSoG follows a hierarchical architecture. An IDS integrated to DIDSoG offers functionalities at a given level of the hierarchy and requests functions from IDSs at other levels. However, DIDSoG differs from the work by Sterne et al. [13] by enabling the integration of heterogeneous IDSs.

Leu et al. [2] propose the use of Globus Toolkit for intrusion detection focusing on Denial of Service (DoS) and Distributed