DCDIDP: A Distributed, Collaborative, and Data-driven IDP Framework for the Cloud

Saman Taghavi Zargar, Hassan Takabi, and James B.D. Joshi

University of Pittsburgh, Pittsburgh, PA, USA
Emails: {stzargar, hatakabi, jjoshi}@sis.pitt.edu

1 Introduction

Recent advances in distributed computing, grid computing, virtualization mechanisms, and utility computing led into Cloud Computing as one of the industry buzz words of our decade. As the popularity of the services provided in the cloud environment grows exponentially, the exploitation of possible vulnerabilities grows with the same pace. Intrusion Detection and Prevention Systems (IDPSs) are one of the most popular tools among the front line fundamental tools to defend the computation and communication infrastructures from the intruders. In this poster, we propose a distributed, collaborative, and data-driven IDP (DCDIDP) framework for cloud computing environments. Both cloud providers and cloud customers will benefit significantly from DCDIDP that dynamically evolves and gradually mobilizes the resources in the cloud as suspicion about attacks increases. Such system will provide homogeneous IDPS for all the cloud providers that collaborate distributively. It will respond to the attacks, by collaborating with other peers and in a distributed manner, as near as possible to attack sources and at different levels of operations (e.g. network, host, VM). We present the DCDIDP framework and explain its components. However, further explanation is part of our ongoing work.

2 Our proposed framework

Our proposed DCDIDP framework comprises of two levels: Infrastructure level and Platform and Software (Virtual machine) level. Infrastructure level itself includes three logical layers: network, host, and general as shown in Figure 1. As it is shown, several collaborative clusters of routers and hosts can be created within network and host infrastructure layers of each cloud provider based on metrics such as physical closeness of components, performance, etc. All the hosts and routers in each of these clusters will share and interact with three local databases for collaborative detection and prevention: *Local Intrusion Assessment Information Base (IAIB)* , *Local Policy & Rule Base* and *Local Audit logs*.

Network infrastructure layer together with host infrastructure layer provide a comprehensive hybrid IDPS or also called global defence mechanism. Distributed and collaborative NIDPSs [1, 2] can be employed on the network infrastructure layer to detect and respond to the attacks properly and in real-time. All the collaborative clusters on network and host infrastructure layers in Figure 1 cooperate with each other to create a comprehensive global version of all the clusters' databases on global infrastructure layer that is shared and used for detection and

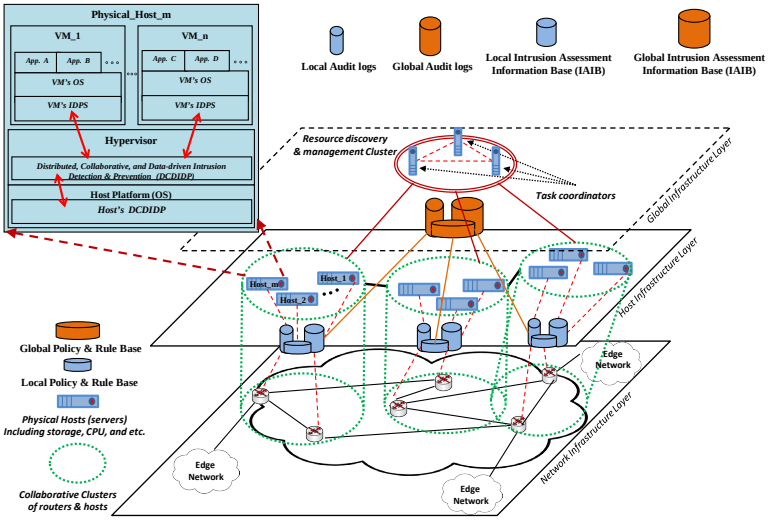

Fig. 1. Cloud provider's DCDIDP framework at different cloud architectural levels

prevention among different cloud providers. Global infrastructure layer is where the collaboration among different cloud providers will be provided through three proposed global databases. Each cluster will update the global databases based on its local databases.

Discovering, assigning, and integrating different services provided through a cloud provider is another responsibility of the global infrastructure layer that is shown as *resource discovery & management cluster*. Task coordinators are synchronized regularly and interact with all the clusters to get the updated status of their current resource availability and to be aware of possible migration of customers' services based on provider's prevention policies.

There can be several physical hosts (e.g. Host_1, Host_2,..., Host_m) within each collaborative cluster each providing different physical resources such as CPU, storage, network, etc. to cloud customers. They also provide virtualized operating systems as well as various APIs to manage physical resources they provide to their customers. Each host can also provide its customers with IDP services in both platform and software (Virtual machine) architectural levels (Figure 1). A cloud customer can be provided with a dedicated virtual machine to run his/her specific applications through cloud hypervisor. In case of providing software level IDP services in our framework, each cloud customer is also provided with an IDPS as an attached service to each virtual machine through the hypervisor. Therefore, each cloud customer is capable of configuring his/her own IDPS with his/her application specifics. In our framework, we provide separate DCDIDP service at the platform level (OS) of a host system as a platform level IDP service. Platform level DCDIDP service is for those cloud customers who rent cloud providers to create, and provide their customers with customized

services or applications. The more granularity we provide in IDP services in the cloud environments, the stronger and the more effective our IDP becomes. At each level, IDPS services have access to both network-based and host-based sensors deployed at the infrastructure level. Additionally, each of the IDPSs in the VMs should report alerts to a host (platform) level DCDIDP, which is responsible for gathering and procesing the alerts of all sensors. Host DCDIDP has access to all of the local databases of the DCDIDP. Host DCDIDP interacts with all of the local databases to update them upon detecting new features of an attack and to access the updated features of previously happened attacks in other hosts. This way each can collaboratively and in a distributed fashion, detect and prevent attacks.

3 Acknowledgement

This work has been supported by NSF award CCF-0720737.

References

1. S.T. Zargar, and J. Joshi, *A Collaborative Approach to Facilitate Intrusion Detection and Response against DDoS Attacks*, 6th Intl Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom'10), Chicago, IL, October 9-12, 2010,
2. T. Znati, J. Amadei, D. R. Pazehoski, and S. Sweeny *On the Design and Performance of an Adaptive, Global Strategy for Detecting and Mitigating Distributed DoS Attacks in GRID and Collaborative Workflow Environments*, Simulation, vol. 83, no. 3, pp. 291–303, 2007.