MALWARE DETECTION IN CLOUD COMPUTING INFRASTRUCTURE

S S Lakshmi Lavanya M, E Kiran Kumar
Assistant Professor, CSE Dept, Sree Dattha Institute of Engineering and Science, Hyderabad.
Assistant Professor, CSE Dept, Guru Nanak Institutions Technical Campus, Hyderabad.

Abstract: Cloud services are prominent within the private, public and commercial domains. Many of these services are expected to be always on and have a critical nature; therefore, security and resilience are increasingly important aspects. In order to remain resilient, a cloud needs to possess the ability to react not only to known threats, but also to new challenges that target cloud infrastructures. In this paper we introduce and discuss an online cloud anomaly detection approach, comprising dedicated detection components of our cloud resilience architecture. More specifically, we exhibit the applicability of novelty detection under the one-class support Vector Machine (SVM) formulation at the hypervisor level, through the utilization of features gathered at the system and network levels of a cloud node. We demonstrate that our scheme can reach a high detection accuracy of over 90% whilst detecting various types of malware and DoS attacks. Furthermore, we evaluate the merits of considering not only system-level data, but also network-level data depending on the attack type. Finally, the paper shows that our approach to detection using dedicated monitoring components per VM is particularly applicable to cloud scenarios and leads to a flexible detection system capable of detecting new malware strains with no prior knowledge of their functionality or their underlying instructions.

1. INTRODUCTION

Cloud data centers are beginning to be used for a range of always-on services across private, public and commercial domains. These need to be secure and resilient in the face of challenges that include cyber attacks as well as component failures and mis-configurations. However, clouds have characteristics and intrinsic internal operational structures that impair the use of traditional detection systems. In particular, the range of beneficial properties offered by the cloud, such as service transparency and elasticity, introduce a number of vulnerabilities which are the outcome of its underlying virtualised nature. Moreover, an indirect problem lies with the cloud’s external dependency on IP networks, where their resilience and security has been extensively studied, but nevertheless remains an issue [1].

The approach taken in this paper relies on the principles and guidelines provided by an existing resilience framework [2]. The underlying assumption is that in the near future, cloud infrastructures will be increasingly subjected to novel attacks and other anomalies, for which conventional signature based detection systems will be insufficiently equipped and therefore ineffective. Moreover, the majority of current signature-based schemes employ resource intensive deep packet inspection (DPI) that relies heavily on payload information where in many cases this payload can be encrypted, thus extra decryption cost is incurred.

Our proposed scheme goes beyond these limitations since its operation does not depend on a-priori attack signatures and it does not consider payload information, but rather depends on
per-flow meta-statistics as derived from packet header and volumetric information (i.e.
counts of packets, bytes, etc.). Nonetheless, we argue that our scheme can synergistically
operate with signature-based approaches on an online basis in scenarios were decryption is
feasible and cost-effective. Overall, it is our goal to develop detection techniques that are
specifically targeted at the cloud and integrate with the infrastructure itself in order to, not
only detect, but also provide resilience through remediation.

At the infrastructure level we consider: the elements that make up a cloud data centre, i.e.
cloud nodes, which are hardware servers that run a hypervisor in order to host a number of
Virtual Machines (VMs); and network infrastructure elements that provide the connectivity
within the cloud and connectivity to external service users.

A cloud service is provided through one or more interconnected VMs that offer access to the
outside world. Cloud services can be divided into three categories based on the amount of
control retained by the cloud providers. Software as a Service (SaaS) retains the most control
and allows customers to access software functionality on demand, but little else. Platform as a
Service (PaaS) provides customers with a choice of execution environment, development
tools, etc., but not the ability to administer their own Operating System (OS). Infrastructure
as a Service (IaaS) relinquishes the most control by providing customers with the ability to
install and administer their own choice of OS and install and run anything on the provided
virtualised hardware; as such, IaaS clouds present the most challenges in terms of
maintaining a properly functioning system. Such a system would ideally be free from
malware and from vulnerabilities that could lead to an attack.

2. RELATED WORK

The intrinsic properties of virtualised infrastructures (such as elasticity, dynamic resource
allocation, service co-hosting and migration) make clouds attractive as service platforms.
Though, at the same time they create a new set of security challenges. These have to be
understood in order to better protect such systems and make them more secure. A number of
studies have addressed aspects of cloud security from different viewpoints (e.g. the network,
hypervisor, guest VM and Operating System (OS)) under various approaches derived either
from traditional rule-based Intrusion Detection Systems (IDSs) or statistical anomaly
detection models.

This paper presents a cloud security solution derived from a sub-domain of anomaly
detection, viz. novelty detection. In this section we firstly review the challenges arising from
the virtualisation embedded within cloud technologies and further discuss background and
related work with respect to anomaly detection in cloud environments. We also present the
architectural context, within which the research presented in this paper is carried out.
3. SYSTEM DESIGN AND DEVELOPMENT

Input Design

Input Design plays a vital role in the life cycle of software development, it requires very careful attention of developers. The input design is to feed data to the application as accurate as possible. So inputs are supposed to be designed effectively so that the errors occurring while feeding are minimized. According to Software Engineering Concepts, the input forms or screens are designed to provide to have a validation control over the input limit, range and other related validations.

This system has input screens in almost all the modules. Error messages are developed to alert the user whenever he commits some mistakes and guides him in the right way so that invalid entries are not made. Let us see deeply about this under module design.

Input design is the process of converting the user created input into a computer-based format. The goal of the input design is to make the data entry logical and free from errors. The error is in the input are controlled by the input design. The application has been developed in user-friendly manner. The forms have been designed in such a way during the processing the cursor is placed in the position where must be entered. The user is also provided with in an option to select an appropriate input from various alternatives related to the field in certain cases.

Validations are required for each data entered. Whenever a user enters an erroneous data, error message is displayed and the user can move on to the subsequent pages after completing all the entries in the current page.

Output Design

The Output from the computer is required to mainly create an efficient method of communication within the company primarily among the project leader and his team members, in other words, the administrator and the clients. The output of VPN is the system which allows the project leader to manage his clients in terms of creating new clients and assigning new projects to them, maintaining a record of the project validity and providing folder level access to each client on the user side depending on the projects allotted to him. After completion of a project, a new project may be assigned to the client. User authentication procedures are maintained at the initial stages itself. A new user may be created by the administrator himself or a user can himself register as a new user but the task of assigning projects and validating a new user rests with the administrator only.

The application starts running when it is executed for the first time. The server has to be started and then the internet explorer in used as the browser. The project will run on the local area network so the server machine will serve as the administrator while the other connected systems can act as the clients. The developed system is highly user friendly and can be easily understood by anyone using it even for the first time.
8. RESULTS

The first and foremost strategy for development of a project starts from the thought of designing a mail enabled platform for a small firm in which it is easy and convenient of sending and receiving messages, there is a search engine ,address book and also including some entertaining games.

When it is approved by the organization and our project guide the first activity, ie. preliminary investigation begins. The activity has three parts:

- Request Clarification
- Feasibility Study
- Request Approval
9. CONCLUSION

In this paper we introduce an online anomaly detection method that can be applied at the hypervisor level of the cloud infrastructure. The method is embodied by a resilience architecture that was initially defined in [4], further explored and which comprises the System Analysis Engine (SAE) and Network Analysis Engine (NAE) components. These exist as sub modules of the architecture’s Cloud Resilience Managers (CRMs), which perform detection at the end-system, and in the network respectively. Our evaluation focused on detecting anomalies as produced by a variety of malware strains from the Kelihos and Zeus samples under the formulation of a novelty detector that employs the one-class Support Vector Machine (SVM) algorithm. Moreover, in order to empower the generic properties of our detection approach we also assess the detection of anomalies by the SAE and NAE during the onset of DoS attacks.

10. REFERENCES


