Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 83 (2016) 1200 – 1206

Procedia Computer Science

The 2nd International Workshop on Mobile Cloud Computing Systems, Management, and Security (MCSMS-2016)

A Cooperative and Hybrid Network Intrusion Detection Framework in Cloud Computing Based on Snort and Optimized Back Propagation Neural Network

Z.Chiba*, N.Abghour, K.Moussaid, A.El omri, M.Rida

Team of Modeling and Optimization of mobile services, Faculty of Sciences, Hassan II University of Casablanca, 20100, Casablanca, Morocco

Abstract

Cloud computing provides a framework for supporting end users easily attaching powerful services and applications through Internet. To give secure and reliable services in cloud computing environment is an important issue. Providing security requires more than user authentication with passwords or digital certificates and confidentiality in data transmission, because it is vulnerable and prone to network intrusions that affect confidentiality, availability and integrity of Cloud resources and offered services. To detect DoS attack and other network level malicious activities in Cloud, use of only traditional firewall is not an efficient solution. In this paper, we propose a cooperative and hybrid network intrusion detection system (CH-NIDS) to detect network attacks in the Cloud environment by monitoring network traffic, while maintaining performance and service quality. In our NIDS framework, we use Snort as a signature based detection to detect known attacks, while for detecting network anomaly, we use Back-Propagation Neural network (BPN). By applying snort prior to the BPN classifier, BPN has to detect only unknown attacks. So, detection time is reduced. To solve the problem of slow convergence of BPN and being easy to fall into local optimum, we propose to optimize the parameters of it by using an optimization algorithm in order to ensure high detection rate, high accuracy, low false positives and low false negatives with affordable computational cost. In addition, in this framework, the IDSs operate in cooperative way to oppose the DoS and DDoS attacks by sharing alerts stored in central log. In this way, unknown attacks that were detected by any IDS can easily be detected by others IDSs. This also helps to reduce computational cost for detecting intrusions at others IDS, and improve detection rate in overall the Cloud environment.

Peer-review under responsibility of the Conference Program Chairs

Keywords: Cloud computing; Network intrusion detection; Back-propagation neural network; Snort; Optimization algorithm

* Zouhair Chiba. Tel.: +212-671-657-123.
E-mail address: chiba.zouhair@gmail.com

Peer-review under responsibility of the Conference Program Chairs
doi:10.1016/j.procs.2016.04.249

1. Introduction

Cloud computing (CC) is rapidly growing computational model in today's IT world. It delivers convenient, on-demand network access to a shared pool of configurable computing resources (e.g. Networks, servers, storage, applications, etc.), "as service" on the internet for satisfying computing demand of users[1].

A recent survey performed by Cloud Security Alliance (CSA) & IEEE, indicates that enterprises across sectors are eager to adopt cloud computing but that security are needed both to accelerate cloud adoption on a wide scale and to respond to regulatory drivers[3]. One of major security issues in Cloud is to detect and prevent network intrusions since the network is the backbone of Cloud, and hence vulnerabilities in network directly affect the security of Cloud. L. Marti from Cyber Security division[6] stated that main concern after data security is an intrusion detection and prevention in the Cloud.

There are principally two types of threads; insider (attackers within a Cloud network) and outsider (attackers outside the Cloud network) considered in Cloud Network.

- Insider attackers: Authorized Cloud users may attempt to gain (and misuse) unauthorized privileges. Insiders may commit frauds and disclose information to other (or modify information intentionally). This poses a serious trust issue. For example, an internal DoS attack demonstrated against the Amazon Elastic Compute Cloud (EC2)[7].
- Outsider attackers: can be called as the network attackers who are able to perform different attacks as IP spoofing, Address Resolution Protocol (ARP spoofing), DNS poisoning, man-in-the-middle, Denial of Service (Dos)/Distributed Denial of service (DDoS) attacks, phishing attack, user to root attack, Port scanning, attack on virtual machine (VM) or hypervisor such BLUEPILL and DKSM through which hackers can be able to compromise installed-hypervisor to gain control over the host, Backdoor channel attacks etc.

These attacks affect the integrity, confidentiality, and availability of Cloud resources and offered services. To address above issues, major Cloud providers (like Amazon ECC, Window Azure, Rack Space, Eucalyptus, Open Nebula etc.) use the firewall. Firewall protects the front access points of system and is treated as the first line of defense. As firewall sniffs the network packets only at the boundary of a network, insider attacks cannot be detected by it. Few DoS or DDoS attacks are too complex to detect using traditional firewall. For example, if there is an attack on port 80 (web service), firewall cannot differentiate normal and legitimate traffic from DoS attack traffic [8]. Thus, use of only traditional firewall to block all the intrusions is not an efficient solution. Another solution is to deploy network based intrusion detection system[10] (NIDS) in Cloud computing. NIDS captures the network packets and applies intrusion detection techniques on captured packets in order to detect networks attacks.

1.1 Our contribution

We propose a new security framework that integrates a cooperative and hybrid-NIDS to Cloud (offering Iaas). We deploy our CH-NIDS at the Front end on Cloud Controller, as well as at on Back end on each processing server (hosting VM) in order to detect both internal and external network intrusions in Cloud Environment. In this framework, we use both the techniques; signature based detection and anomaly based detection. Snort as a signature based detection is used to detect known attacks, while for detecting network anomaly, we use an optimized Back Propagation Neural network (BPN). Several researchers used BPN approach for detection intrusion attacks, because it has shown good capability in detecting attacks[2]. But, according to many researches, BPN has the following weaknesses[5, 12]:

- Slow detection speed.
- Low detection accuracy.
- Easy to fall into local minimum value.
- Slow convergence speed.

In order to solve the problems above, we propose to optimize the BPN by using an optimization algorithm. Combining signature based detection and anomaly detection in our NIDS module improves detection accuracy; since they are complimenting each other. In addition, the signature based detection technique is applied prior to anomaly detection, which reduces the computational cost. BPN classifier has to detect only unknown attacks, because known attacks are already detected by Snort and denied. By using central log of malicious packets detected,