Journal of Network and Computer Applications 36 (2013) 42–57

Contents lists available at SciVerse ScienceDirect

Journal of Network and Computer Applications

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

Review

A survey of intrusion detection techniques in Cloud

Chirag Modi [a],*, Dhiren Patel [a], Bhavesh Borisaniya [a], Hiren Patel [b], Avi Patel [c], Muttukrishnan Rajarajan [c]

[a] NIT Surat, Gujarat, India
[b] S.P. College of Engineering, Gujarat, India
[c] City University London, UK

ARTICLE INFO

Article history:
Received 3 January 2012
Received in revised form
15 May 2012
Accepted 16 May 2012
Available online 2 June 2012

Keywords:
Cloud computing
Firewalls
Intrusion detection system
Intrusion prevention system

ABSTRACT

In this paper, we survey different intrusions affecting availability, confidentiality and integrity of Cloud resources and services. Proposals incorporating Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) in Cloud are examined. We recommend IDS/IPS positioning in Cloud environment to achieve desired security in the next generation networks.

Contents

1. Introduction . . . 43
2. Intrusions to Cloud systems . . . 43
   2.1. Insider attack . . . 43
   2.2. Flooding attack . . . 43
   2.3. User to root attacks . . . 43
   2.4. Port scanning . . . 43
   2.5. Attacks on virtual machine (VM) or hypervisor . . . 43
   2.6. Backdoor channel attacks . . . 44
3. Firewalls: common solution to intrusions . . . 44
4. IDS and IPS techniques: evolution . . . 44
   4.1. Signature based detection . . . 44
   4.2. Anomaly detection . . . 45
   4.3. Artificial neural network (ANN) based IDS . . . 45
   4.4. Fuzzy logic based IDS . . . 45
   4.5. Association rule based IDS . . . 45
   4.6. Support vector machine (SVM) based IDS . . . 46
   4.7. Genetic algorithm (GA) based IDS . . . 46
   4.8. Hybrid techniques . . . 46
5. Various types of IDS/IPS used in Cloud computing . . . 47
   5.1. Host based intrusion detection systems (HIDS) . . . 47
   5.2. Network based intrusion detection system (NIDS) . . . 49
   5.3. Distributed intrusion detection system (DIDS) . . . 50
   5.4. Hypervisor-based intrusion detection system . . . 51
   5.5. Intrusion prevention system (IPS) . . . 52
   5.6. Intrusion detection and prevention system (IDPS) . . . 55

* Corresponding author. Tel.: +91 9408883560.
E-mail address: cnmodi.956@gmail.com (C. Modi).

1084-8045/$ - see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.jnca.2012.05.003

6. Conclusions 56
References 56

1. Introduction

Cloud computing aims to provide convenient, on-demand, network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services), which can be rapidly provisioned and released with minimal management effort or service provider interactions (Mell and Grance, 2011). Cloud provides services in various forms: Software as a Service-SaaS (e.g. Google apps, 2011), Platform as a Service-PaaS (e.g. Google app engine (2011)), Microsoft's Azure (Azure services platform, 2011)) and Infrastructure as Service-IaaS (e.g. Amazon web services, 2011(AWS); Eucalyptus, 2011; Open Nebula (Opennebula, 2011)).

As Cloud services are provisioned through the Internet; security and privacy of Cloud services are key issues to be looked upon. International Data Corporation (IDC) survey (Gens, 2009) showed that security is the greatest challenge of Cloud computing. The recent Cloud computing security white paper by Lockheed Martin Cyber Security division (Martin, 2010) shows that the major security concern after data security is intrusion detection and prevention in Cloud infrastructures. Cloud infrastructure makes use of virtualization techniques, integrated technologies and runs through standard Internet protocols. These may attract intruders due to many vulnerabilities involved in it.

Cloud computing also suffers from various traditional attacks such as IP spoofing, Address Resolution Protocol spoofing, Routing Information Protocol attack, DNS poisoning, Flooding, Denial of Service (DoS), Distributed Denial of Service (DDoS), etc. For e.g. DoS attack on the underlying Amazon Cloud infrastructure caused BitBucket.org, a site hosted on AWS to remain unavailable for few hours (Brooks, 2009). Computing-cost using current cryptographic techniques cannot be overlooked for Cloud (Chen and Sion, 2010). Firewall can be a good option to prevent outside attacks but does not work for insider attacks. Efficient intrusion detection systems (IDS) and intrusion prevention systems (IPS) should be incorporated in Cloud infrastructure to mitigate these attacks.

Rest of the paper is organized as follows: Section 2 discusses various attacks applicable to Cloud environment. Traditional firewalls as a security solution are discussed briefly in Section 3. Section 4 presents various techniques for IDS/IPS. Section 5 surveys existing IDS/IPS types and examines Cloud specific work on IDS with conclusion and references at the end.

2. Intrusions to Cloud systems

There are several common intrusions affecting availability, confidentiality and integrity of Cloud resources and services.

2.1. Insider attack

Authorized Cloud users may attempt to gain (and misuse) unauthorized privileges. Insiders may commit frauds and disclose information to others (or modify information intentionally). This poses a serious trust issue. For example, an internal DoS attack demonstrated against the Amazon Elastic Compute Cloud (EC2) (Slaviero, 2009).

2.2. Flooding attack

In this attack, attacker tries to flood victim by sending huge number of packets from innocent host (*zombie*) in network. Packets can be of type TCP, UDP, ICMP or a mix of them. This kind of attack may be possible due to illegitimate network connections.

In case of Cloud, the requests for VMs are accessible by anyone through Internet, which may cause DoS (or DDoS) attack via *zombies*. Flooding attack affects the service's availability to authorized user. By attacking a single server providing a certain service, attacker can cause a loss of availability of the intended service. Such an attack is called direct DoS attack. If the server's hardware resources are completely exhausted by processing the flood requests, the other service instances on the same hardware machine are no longer able to perform their intended tasks. Such type of attack is called indirect DoS attack.

Flooding attack may raise the usage bills drastically as the Cloud would not be able to distinguish between the normal usage and fake usage.

2.3. User to root attacks

Here, an attacker gets an access to legitimate user's account by sniffing password. This makes him/her able to exploit vulnerabilities for gaining root level access to system. For example, Buffer overflows are used to generate root shells from a process running as root. It occurs when application program code overfills static buffer. The mechanisms used to secure the authentication process are a frequent target. There are no universal standard security mechanisms that can be used to prevent security risks like weak password recovery workflows, phishing attacks, keyloggers, etc.

In case of Cloud, attacker acquires access to valid user's instances which enables him/her for gaining root level access to VMs or host.

2.4. Port scanning

Port scanning provides list of open ports, closed ports and filtered ports. Through port scanning, attackers can find open ports and attack on services running on these ports. Network related details such as IP address, MAC address, router, gateway filtering, firewall rules, etc. can be known through this attack. Various port scanning techniques are TCP scanning, UDP scanning, SYN scanning, FIN scanning, ACK scanning, Window scanning etc. In Cloud scenario, attacker can attack offered services through port scanning (by discovering open ports upon which these services are provided).

2.5. Attacks on virtual machine (VM) or hypervisor

By compromising the lower layer hypervisor, attacker can gain control over installed VMs. For e.g. BLUEPILL (Rutkowska, 2006), SubVir (King et al., 2006) and DKSM (Bahram et al., 2010) are some well-known attacks on virtual layer. Through these attacks, hackers can be able to compromise installed-hypervisor to gain control over the host.

New vulnerabilities, such as zero-day vulnerability, are found in Virtual Machines (VMs) (NIST: National vulnerability database, 2011) that attract an attacker to gain access to hypervisor or other installed VMs. Zero-day exploits are used by attackers before the