Honeypots For Cloud Computing
Eduardo Henrique de Carvalho Moura & Zair Abdelouahab
Federal University of Maranhão – UFMA
CCET/DEEE/UFMA
Campus do bacanga
São Luis MA 6500 080 Brazil
eduardohcmoura@gmail.com, zair@dee.ufma.br

ABSTRACT
With the advance of internet use and the search for greater mobility, cloud computing is becoming an option for those who want to access their data and other services from anywhere. With the increased use and adoption of this technology by large companies, security has become a big issue to their growth. Cloud computing facilities (public as well as private) are becoming targets of numerous malicious attacks.
In this paper, we provide a survey of cloud computing, highlighting security strategies using honeypots. We present some models of honeypots available in the literature and conclude the paper with a critical analysis.

Keywords
Honeypots, Cloud Computing, Security, Virtualization
1. INTRODUCTION

Cloud computing is the future trend of computing. With cloud computing, it is no longer needed to install various software in a personal device to perform any task, such as editing pictures, videos, and office programs, since everything will be accessible through the Internet as a service. If anyone wants any of these services, simply he needs to register with the service provider, and then access the cloud to perform any activity, save the data generated in the cloud itself and access them from anywhere just by using internet connection.

In order to build complex IT infrastructures, the user usually is responsible for installing, configuring, replacing and updating software and hardware which may soon obsolete, outsourcing of computing platforms is a solution for users to deal with the problems with the infrastructure IT. In cloud computing IT resources are provided as a service, allowing users to access it without the need for knowledge on the technology used. Thus, users and companies began to access services on demand, independent of location, which increases the amount of available services [1].

Large companies like Amazon, Google, Microsoft and others are investing high and striding credit for this trend. Due to this high investment, the development of systems and cloud computing services has increased, giving more available options and available solutions for users and luring them increasingly using cloud-based applications [2].

Cloud computing has its services divided into three classes in which which resources have different levels of abstraction and service model offered by the provider. The level of abstraction layer referring to the real system is abstracted by the cloud. The three classes of services are named as: Infrastructure as a Service (IaaS) in the lower layer; Platform as a Service (PaaS), in the intermediate layer, and Software as a Service (SaaS), in the upper layer [3].

What still restricts the adoption of cloud computing is that many companies fears the problems of security such as integrity, confidentiality and availability of data and applications in the cloud. To choose a security solution for the cloud, it is necessary to decide which type of model where security is to be provided for the cloud. Currently, there are three models: public, private, and hybrid [4] clouds.

Tais nuvens funcionam como uma grade computacional que segundo Techtarget (2012), grade de computação (ou a utilização de uma grade computacional) é a aplicação dos recursos de muitos computadores numa rede para um único problema, ao mesmo tempo e normalmente para um problema científico ou técnica que requer um grande número de ciclos de processamento ou de acesso a grande quantidades de dados [10]. Assim uma nuvem pode ser formada por um ou vários nós computacionais.

In cloud computing there there are different roles, each of which has its own importance and responsibility, and access profile for the different users that are part or involved in a cloud computing solution. For better understanding of cloud computing, we can classify the models of actors according to the roles performed [11].

Developers use the resources provided by the providers and provide services to end users. This kind of organization helps us to define the roles for the actors and their different interests. Actors can take several roles at the same time according to the interests, and only the provider provides support to all service models [12]. This organization creates greater security and better policy group which is a safety plus for cloud users.

Besides a good definition of roles in the cloud and creating policies for access group other well-defined strategies to ensure the security of cloud computing has been adopted, such as: use of IDS (Intrusion Detection Systems) [13], firewall and antivirus.

All these strategies are very useful against already known threats, but many new forms of attacks and threats to clouds are created daily. For this purpose, the honeypots as a tool for security of network systems has been greatly shown in [6], [7] and [8] and recently used for clouds as in [5] and [9]. In this paper, we present a survey on honeypots for Cloud Computing environment. The paper is organized as follows. Section 1 introduces the work. Section 2 gives a brief background on security, honeypots and virtualization. Section 3 describes the existing works on honeypots for cloud computing. Section 4 does a comparative study on honeypots for cloud computing. Finally, section 5 gives some concluding remarks.

2. SECURITY FOR CLOUD COMPUTING AND BACKGROUND

The cloud is a metaphor for the Internet or communications infrastructure between the architectural components based on an abstraction that hides the infrastructure complexity. Each part of the infrastructure is provided as a service and these are usually allocated in data centers using shared computing and storage and hardware [14].

Security in cloud computing is a relatively a new field of technology. It has gained much importance due to the acceptance and use of this technology by big companies like Amazon, Google, Microsoft and others [2]. Virtualização techniques are offered using Virtual Machine Manager (hypervisors), where processors, disk drives and storage networks are simulated. With virtualization, it is possible to operate different instances sharing the same physical servers. However, this makes the cloud computing environment more vulnerable because malicious users can steal data by means of spy programs, or monitor the different virtual machines running on the same server [5].

2.1 Problems Faced By Cloud Providers

In [5], major problems faced by cloud computing providers are reported such as: ensuring that the infrastructure is secure, the customer data and applications are protected, ensure that data of a customer are adequately separated from data of...
others to avoid data leaks or access by third parties, and ensure that the applications available as a service via the cloud are secure.

2.2 Problems Faced By Clients

Again in [5], the main problems faced by customers using cloud computing are reported such as: abstraction of the cloud architecture, control of instances, the privacy of their data and attacks suffered by their instances.

2.3 Problems Of Cloud Computing

Cloud computing has problems that are inherent to the technology such as confidentiality, availability, privacy and integrity of customer data [15].

The issue of confidentiality [15] is a problem due to: the service provider knows where sensitive user data are in the cloud; it has the privilege to access and collect confidential data from users; the cloud service provider can understand the meaning of users data. In [16] confidentiality is placed as a major concern for users of cloud computing because there are serious risks of unauthorized use of user data by service providers.

Other problems such as identification and authentication, authorization, integrity, non-repudiation and availability are issues that must be taken into consideration when choosing a solution for cloud computing.

2.4 Virtualization Layer

One of the technologies that enabled the development of cloud computing is virtualization, where it is possible the creation of virtual machines (Virtual Machine - VM) running operating systems on the same hardware [17]. The Virtual Machine Monitor or hypervisor is the layer responsible for abstracting the hardware; it intermediates the VMs. VMs in turn act as replicas of this hardware and may or may not contain all the features such as processing power and disk space on the host hardware [18]. Thus, VMs are copies of the host hardware, but each one has its own operating system and isolated applications.

2.5 HONEYPOTS

Honeypots are defensive security systems such as IDS (intrusion detection systems) and Firewalls. They simulate the network services that are available in the network to attract intruders [5]. They may be physically installed or virtualized in the network [19]. They may be deployed depending on a model considering the advantages and disadvantages in relation to the quantity and quality of the captured data, types of attacks that can store information and the risks of a honeypot may present when it is used to attack others after being compromised.

Honeypots are classified according to the degree of their interaction with the attacker. They can be: low, medium or high interaction honeypots[5] [19]. Honeypots of low and medium interaction have activities and services configured in order to meet the interactions of malicious user. High interactivity honeypots are deployed in systems with real services (production machines); they may present high risks to the services when they are compromised and used as a starting point for making attacks. These are complex to configure and they can generate a greater amount of interaction logs.

In [20] Spitzner lists some advantages of using honeypots in a network such as collecting information on the type of attacks, shifting the focus of attacker from the real service, and use these systems to attract the attackers and thus acquiring more information on the attacker.

3. USE OF HONEYPOT IN CLOUD COMPUTING

As in traditional networking systems, honeypot technology is applied in cloud computing to assist with systems protection and information collection on the types of attacks, thus logs can be maintained to improve the security of cloud servers and the computational instances.

Some studies show different uses of this technology to cloud computing as in [5], [9], [23] and [24]. Some tools that may be used to facilitate the creation and management of the honeypots such as Honeyd [21] and Sebek [22].
3.1 Automatic Detection of XSS Attacks Using Snort signatures and ACLs Through a Honeypot Based On the Cloud

In [5], a system of automatic detection of XSS attacks by generating Snort signature is developed to block similar future attacks using access control lists (ACL). For that purpose, a low-interaction honeypot is installed in a computational cloud to simulate a web server and is exposed to XSS attacks.

The honeypot is configured with Honeyd instance that is installed in another access group different from the production group thus reducing the risk of an attack have some effect on them or the attacker have access to data of Production instances. Attacks directed to the cloud are honeypot that do not directly aimed at machines in the production network, but the cloud.

This security model for the cloud consists of an Intrusion Detection System (IDS) which makes captures patterns of attacks, the packets that pass through the IDS reach the second session of the system that consists of a sensor security (honeypot) disposed within the cloud infrastructure that is capable of detecting unknown threats. Packets passing through the hypervisor are checked to see whether they are intended for any virtual machine of the cloud. If they are not, then they are directed to the honeypot. Figure 1 shows the design of the architecture proposed by [5].

Snort used in [5] has six basic sessions in its configuration file: variable definitions, configuration parameters pre-processor configuration, output configuration module, new action types and configuration rules, used to generate the ACLs from the honeypot logs.

Honeypot logs are also used to generate the signatures of XSS (Cross-site scripting) for this specific fields found in the honeypot log file and compare them with well-known brands "random_strings <script> </script>". New signatures are inserted in the Snort signature file thus automating the process of updating and defense against new attacks.

3.2 Honeypot as a Service in the Cloud

In [9], it demonstrates an implementation model of a Honeypot in a cloud environment to provide safety and profit to a business. For an efficient operation of this model of a honeypot for the cloud, it has an independent implementation from the software used to configure the cloud environment, thus creating a service named Haas (Honeypot as a Service). The paper [9] states that a cloud platform independent honeypot is the best way to improve cloud security, since the nodes of the honeypot controls are separate from the cloud controller as shown in Figure 2.

The implementation has the following components:

- Cloud Controller: is the central control unit to a cloud environment. It is used to manage and expose virtualized resources (machines, network and storage) through APIs to the user;
- Controller cluster is present in a cloud environment to control various clusters similar to a Virtual Machine Manager (VMM) controlling the execution of multiple virtual machines running on the nodes. It is associated with the storage controller that is used to provide data storage block level. Under each cluster controller supervises a group node controllers that are used to manage the initialization, execution and termination of services provided by virtual machine instances;
- Honeypot Controller: is a controller node that is separate from others providing real services; it provides a separate cluster controller for honeypot instances. This separation is highly essential because the commitment of...
honeypot instances should not affect other controllers and instances running in the cloud. This cluster controller where honeypots are running is called a honeypot controller. There may be many simulated cases corresponding instances running in the cloud to provide a high-interaction honeypot;

- Filter and Redirection Engine-RES aims to separate malicious traffic from legitimate users and redirect them to the controller honeypot. The traffic is analyzed with respect on some flagged signatures and false doors running on the honeypot;
- Storage system logs stores all the records information about the attackers and registers them in FRE before the traffic is redirected to the honeypot controller. These records are stored in a centralized storage system log on the cloud controller and usually contain information about the attacker's IP address, type, date, time and frequency of attack.

Figure 2 shows the honeypot model proposed in [9].

This model uses a Filter and Redirection Engine (FRE) to redirect all malicious traffic destined for a particular real instance to the honeypot. The latter is configured to interact with the attacker by providing him false instances running in the cloud, and storing all information on the source of traffic. The engine must be implemented with efficient algorithms since all traffic directed to the cloud must be analyzed. Its operation is similar to an IDS that analyzes the packet by comparing it with known patterns of signatures that may indicate the type of attack and if necessary the controller honeypot discards the packet. Figure 3 shows a controller with cloud storage and RES System Log.

When the attacker is not detected by FRE, the former can gain access to the resources and for this reason, the model should be implemented along with other forms of defense such as an IDS.

An advantage of the proposed model in [9] is that the controller honeypot implemented as a separate cluster controller can use instances that simulate real systems thereby building high-interaction honeypot without endangering the structure of the cloud and the data stored on it. This model focuses on the security of cloud instances since all interaction is about communication between the instances. However, the Haas service is available to the user of the cloud as an extra service which the cloud provider can charge for the service depending upon the sophistication of the honeypot and the type of simulation.
3.3 Enhancing Security in Cloud Computing

The work [23] proposes a model to increase security in the cloud where the focus is not the instances within the cloud but the data stored by users. It proposes two (02) cycles of authentication and disassociation of the team responsible for encryption and the team of developers of the cloud. Thus, when a user who wants access has to do two rounds of login authentication. The first round is for authentication in the cloud and the second is to get the data encryption key. The proposed model provides a honeypot that simulates security user data; thus if a malicious user succeeds to enter the cloud, he will not have access to actual user data since he does not have the encryption key.

![Fig 4: Proposed Architecture [23]](image)

This concern is made thinking about the confidentiality of client data from a provider of cloud storage since employees of this provider may have access to client data in an unauthorized manner since they have access to the cloud environment as administrators.

In this model, when a user (employee or anonymous) wants to store or access a data, he should have to register with the organization to get a username and a password for authentication purposes. To access the data, a user has to authenticate with its username and password. Then, the authentication system of the cloud provider verifies the username and password. If the user and password are valid, the encryption provider checks whether the user has access to that data or directory. If the user has no access right, then its request is redirected to the honeypot. Thus, unauthorized users or hackers that invade an account of a particular user receives data from the fake database honeypot. The honepot can then collect more information from the malicious cloud user. Figure 4 [23] shows the proposed architecture in which the system has two real databases and one fake database.

3.4 Integrated Intrusion Detection and Prevention System with a Honeypot

A system model for protecting a cloud computing facility is shown in [24], and consists of an IDPS (Intrusion Detection and Prevention System) and a low-interaction honeypot.

The intrusion detection system based on signature is used to differentiate between normal traffic and possible attacks. The IDS is distributed across the virtual network to monitor system activity and control the packet traffic in the network to filter the malicious packets from suspected sources [24]. This system works by configuring a firewall, which transfers malicious traffic to a honeypot server. The honeypot acts as a surveillance tool and attraction to intruders. It is a computer or a local network, which is isolated from real production network containing information giving to him an illusion that are valuable to attract the attacker, but are actually false. The work focuses on the security level of the Infrastructure as a Service (IaaS).
The proposed honeypot model of [24] is installed behind the firewall to detect possible failures of the latter, to allow the IDPS to read the packets and compare them with the signatures of its database and possibly introduce new rules in the firewall that redirects the packet to the controller honeypot. In addition, the proposed model can detect abnormal behavior according to the detection method based anomaly. It also produces an alarm and saves the event as a new threat in order to provide new firewall rule.

The firewall is a useful part for the honeypot project. It is able to provide storage capabilities of the activities and identify an intruder trying to break into a honeypot. With an internally installed honeypot, it is also possible to detect a misconfigured firewall that forwards unwanted traffic from the Internet to the internal network. The main idea for the deployment of a honeypot behind a firewall is to detect internal attacks.

Figure 6 shows a conceptual view of the cloud with the IDS honeypot.

4. ANALYSIS AND COMPARISONS

Table 1 shows different characteristics of different models of honeypots which were analyzed.
Table 1: Honeypots for Cloud Computing

<table>
<thead>
<tr>
<th>Characteristics</th>
<th>Low/Medium Interactivity</th>
<th>High Interactivity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual</td>
<td>[5], [9], [23] e [24]</td>
<td></td>
</tr>
<tr>
<td>Real</td>
<td>[9]</td>
<td></td>
</tr>
<tr>
<td>With targeted traffic</td>
<td>[5], [23] e [24]</td>
<td>[9]</td>
</tr>
<tr>
<td>Located in a DMZ</td>
<td>[5], [23] e [24]</td>
<td>[9]</td>
</tr>
<tr>
<td>Located with Production services</td>
<td>[9]</td>
<td></td>
</tr>
<tr>
<td>protection of instances</td>
<td>[5], [9] e [24]</td>
<td>[9]</td>
</tr>
<tr>
<td>User Protection</td>
<td>[23]</td>
<td></td>
</tr>
<tr>
<td>Works with an IDS</td>
<td>[5][9][24]</td>
<td>[9]</td>
</tr>
<tr>
<td>Works with ACL</td>
<td>[5]</td>
<td>[9]</td>
</tr>
</tbody>
</table>

In [5] we have a low-interaction honeypot that is located within the cloud simulating an instance of a web server; the traffic is directed to it through the firewall, since packets with possible XSS attacks are recognized by the IDS. To create a honeypot, the Honeyd framework [21] is used to manage the honeypot. In [9] and [24] the honeypot is part of a security system where the logs are used to generate signatures for new attacks and ACLs are inserted into a firewall to block packets that originate from addresses that have been identified as points of departure attacks.

Among the works that were analyzed, the work in [9] proposes the implementation of a high-interaction honeypot that does not simulate only an instance but a cluster or part of the cloud infrastructure. It also proposes a low interactivity honeypot inside the cloud in order to protect users instances. This type of honeypot is made available as Haas service (Honeypot as a Service).

The work [23] is the only one that simulates a service to provide security for users by creating a fake database whenever a user is identified as unauthorized or unauthenticated.

5. CONCLUSION

This paper discussed examples of works related to the use of honeypots for cloud computing security. We have shown different approaches for providing honeypots within VLANs of a cloud computing facility. We have also showed about the advantages and disadvantages of low / medium and high interaction honeypots.

ACKNOWLEDGMENTS

Our thanks to FAPEMA and CAPES for their Financial support.

REFERENCES


