Intrusion Detection Types in the Cloud

Florent Gontharet Naghmeh Moradpoor
School of Engineering, Computing and Applied Mathematics
University of Abertay Dundee
DUNDEE, DD1 1HG, UK

ABSTRACT

Cloud computing is a new way of providing computer-related services over the Internet. To meet the needs, the architecture is specific, and allow an important scalability and redundancy.

As the tendency spreading, the risks are growing for the data stored by the providing companies, turning them into valuable targets from an attacker's point of view.

To detect and prevent attacks, firewalls are efficient regarding outsiders, but the attack could be from the inside, as a user trying to gain privileges. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are great tools against attacks from outside, and from inside as well.

We will start by a review of some main attacks that can occur, and continue to approach the subject using multiple paths, as there are plenty, providing their own solution, and see what makes them adapted to a situation.

Keywords

Cloud computing; Firewall; IDS; IPS;

1. INTRODUCTION

Cloud computing can designate a lot of different services: Infrastructure-as-a-Service (IaaS, e.g. Amazon Web Service), Platform-as-a-Service (PaaS e.g. Microsoft Azure), Software-as-a-Service (SaaS e.g. Oracle Taleo). It is made in order to provide users easy and accessible computing resources to meet their needs. As the time to set up a new machine has decreased and the fact that there is no maintenance cost, the trend has been set and companies are now heading for those solutions.

As it uses Internet to provide services, Cloud computing security already involve all the issues related to Internet, such as malwares, hackers, privacy, etc. And plenty of attacks can target it: Denial-of-Service (DoS), Distributed-DoS (DDoS), Man-in-the-Middle (MITM), DNS poisoning, etc. Finally, because it centralizes all the data from different companies, it represents a valuable target.

Firewalls are protecting the border of the network, but if a legitimate user starts an attack from the inside, it won't be detected, and it represents a serious threat.
This document is organized as follows: we will see some important threats against cloud ccomputing architectures in part 3.1. Next we will approach the different existing Cloud IDS/IPS solutions, in order to examine them and analyze the answer they provide to the security issues, in part 3.2.
The background presents an overview of the cloud computing security landscape.

2. BACKGROUND

Cloud computing involvement in people's lives is growing. Privacy is a nowadays' concern, and by definition, privacy should includes security. At first, as we can read from [12] Srinivasan, S. 2014, Cloud Computing Basics, Springer Verlag, DE., security is a problem for the hosting company itself: the main expectations from a customer are the availability and the security of their data. In a cloud computing architecture, the security of the data is almost entirely managed by the hosting company.

Second, Rountree, D. & Castrillo, I. 2013, Basics of Cloud Computing, Syngress. [10] explains that security based on tests is based on current knowledge of vulnerabilities, forgetting the zero-day exploits and other vulnerabilities exposure. Explaining that it is not enough to have security controls, they have to be effective as well.

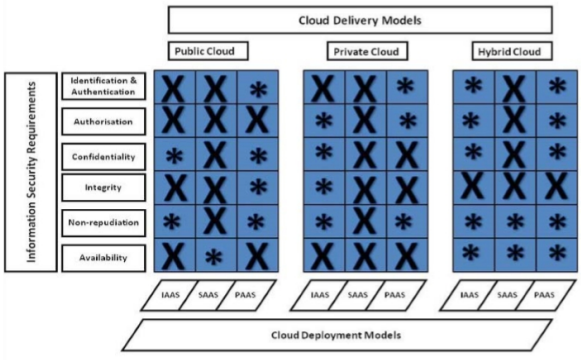

Figure 1 – Cloud security needs per infrastructure

As shown in Baiardi, F., Baiardi, F., Sgandurra, D. & Sgandurra, D. 2010, "Securing a Community Cloud", IEEE, pp. 32. [3], the architecture and the needs defines the policies, the architecture, and the behaviors. Also, it is not easy to provide a unique, adaptable answer meeting all the needs, and specificity.

3. METHOD

3.1 Main threats

3.1.1 Denial-of-Service (DoS)

As the services are provided through the Internet, they are accessible by everyone, and an attacker can use it to start sending an important amount of traffic, in order to make it busy, until it does not respond anymore. The DDoS consist in the same aim, using multiple computers around the world at the same time, targeting the same server [5]. Usually those computers are infected and therefore part of a botnet, they are called zombies.

3.1.3 Port Scanning

In order to perform an attack, important information can be found on the network. A port scanner will verify what protocols the server is using, and its operating system. It makes the attack way easier. [6] Port scanning can be detected by an IDS, or block by a firewall if launched from outside the network.

3.1.4 Insider Attack

Authorized users can try to obtain more information than they should, gain access, perform different kind of attacks, and even delete information. It is not detected by the firewall, as already inside the network, and can be detected y an IDS.

3.1.5 Hypervisor

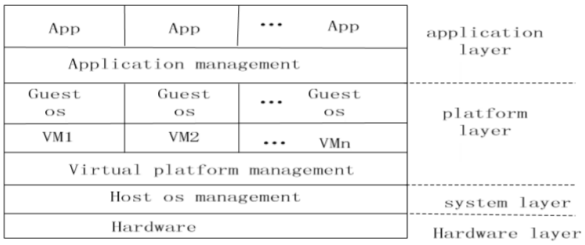

Figure 2 – Architecture of a server

In order to provide scalability, the architecture has moved to a virualization of the machines (VM), and a sharing of resources. To virtualize those machines, the servers are using a layer called hypervisor. The role of the hypervisor is to ensure every virtual host is separated from each other. As operating systems are not perfect, hypervisors are not, and security breaches might appear [14]. Attack against the hypervisor wont be detected by a firewall or a standard IDS, we will approach the question in 3.2.4.

3.2 Different IDS approaches

An IDS is a system that will analyze all the traffic on the network. They will compare them against their database, and decide whether or not it's an attack, in order to alert an administrator, or an IPS, to stop the intrusion. They are two type of IDS database: rules or signature based. Depending on how the IDS will analyze it. An anomaly-based IDS will detect more false positives, but will be more efficient as well as a signature-based IDS, that won't detect an attack if there is a small change in the packet's signature. The following is about IDS types, that can be implemented in a cloud computing architecture.

3.2.1 Host-based

A host-based IDS is a software running on the system that analyzes kernel and file system changes, among other suspicious behaviors. The settings are really important to monitor the right files. A knowledge-based IDS detects known attacks, and behavior-based IDS will detect unknown attacks and communicate with the others to keep them up-to-date. The false positives are low and false negatives as well [13].

3.2.2 Network-based

A network-based IDS is a software run on a server that will analyze all the packets, in order to detect any malicious traffic. But it has a really limited knowledge about the hosts, and encrypted streams cannot be analyzed. It is really effective for (D)DoS attacks, and can be used to detect ARP Spoofing as well [1]. A network-based IDS has capabilities to detect intrusions based on real-time and behavior observations. Also, it keeps a list of events.

3.2.3 Distributed IDS

A distributed IDS is multiple host or network based IDS called mobile agents, all communicating with a main server [7]. Also, the main server knows everything about the network and the clients, and has a common database for all of them. In case of a high-level alert, it can learn and write rules.

3.2.4 Hypervisor-based

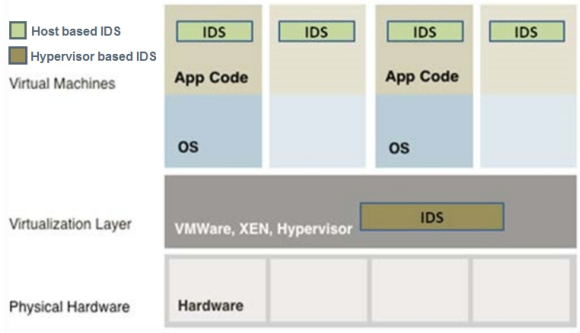

Figure 3 – Host and Hypervisor based IDS

A hypervisor-based IDS is a host-based IDS, with the difference than instead being in the operating system of each client, it is invisible and analyzing streams passing from the operating system through the hardware. It is useful against a lot of different attacks, and can even provide performance signature to detect attacks [8].

3.2.5 Data mining-based

Data mining can be applied to IDS in order to generate profiles and detect e.g. masquerades [9]. An anomaly and misuse detection provide alerts in case of a match.

3.2.6 Intrusion Detection and Prevention System (IDPS)

An IDPS is a system not only detecting, but preventing intrusions. For that, it includes the detection part of an IDS, applied to an IPS, Intrusion Prevention System. It is not only able to send alerts, but it can also block them. For that, it runs a real-time analysis of the packets on the network [11].

4. CONCLUSION

As we can see, IDS is not one easy thing to implement, as security isn't as well. Cloud computing is still in some early ages and there are already plenty of ways to approach the problem to get the solution required. As there is no perfect one, a reflexion has to be made to meet the needs of the specificity of the architecture.

It is an important subject evolving fast, security tools have to be implemented smartly and in order to be efficient. A bad tool, or a bad implementation could open more breaches than it closes.

As shown in Cha, B. & Kim, J. 2013, "Security tactics for secured cloud computing resources", pp. 473.[4], IDS can be used with honeypots, to observe the attacker or with an IPS and block him, as shown in Alqahtani, S.M., Balushi, M.A. & John, R. 2014, "An Intelligent Intrusion Prevention System for Cloud Computing (SIPSCC)", IEEE, pp. 152.[2].

Finally, cloud computing security is offering great challenges and solutions, and the improvement in this field will continue to help cloud computing to reach more companies.

5. REFERENCES

[1] Alqahtani, S.M., Balushi, M.A. & John, R. 2014, "An Intelligent Intrusion Detection System for Cloud Computing (SIDSCC)", IEEE, pp. 135.

[2] Alqahtani, S.M., Balushi, M.A. & John, R. 2014, "An Intelligent Intrusion Prevention System for Cloud Computing (SIPSCC)", IEEE, pp. 152.

[3] Baiardi, F., Baiardi, F., Sgandurra, D. & Sgandurra, D. 2010, "Securing a Community Cloud", IEEE, pp. 32.

[4] Cha, B. & Kim, J. 2013, "Security tactics for secured cloud computing resources", pp. 473.

[5] Darwish, M., Ouda, A. & Capretz, L.F. 2013, "Cloud-based DDoS attacks and defenses", Infonomics Society, pp. 67.

[6] Deshpande, P., Aggarwal, A., Sharma, S.C., Kumar, P.S. & Abraham, A. 2013, "Distributed port-scan attack in cloud environment", IEEE, pp. 27.

[7] Dhage, S., Meshram, B., Rawat, R., Padawe, S., Paingaokar, M. & Misra, A. 2011, "Intrusion detection system in cloud computing environment", ACM, pp. 235.

[8] Nikolai, J. & Wang, Y. 2014, "Hypervisor-based cloud intrusion detection system", IEEE, pp. 989.

[9] Pratik, P.J. & Madhu, B.R. 2013, "Data mining based CIDS: Cloud intrusion detection system for masquerade attacks [DCIDSM]", IEEE, pp. 1.

[10] Rountree, D. & Castrillo, I. 2013, Basics of Cloud Computing, Syngress.

[11] Scarfone, K. & Mell, P., 2007, “Guide to Intrusion Detection and Prevention Systems (IDPS), US NIST.

[12] Srinivasan, S. 2014, Cloud Computing Basics, Springer Verlag, DE.

[13] Wang, H. & Zhou, H. 2012, "The Research of Intrusion Detection System in Cloud Computing Environment" in Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 45-49.

[14] You, P., Peng, Y., Liu, W. & Xue, S. 2012, "Security Issues and Solutions in Cloud Computing", IEEE, pp. 573.