Journal of Advanced & Applied Sciences (JAAS)
Volume 03, Issue 05, Pages 152-158, 2015
ISSN: 2289-6260

Security Everywhere Cloud: An Intensive Review of DoS and DDoS Attacks in Cloud Computing

Aws Naser Jaber [a,b], Mohamad Fadli Bin Zolkipli, [c,*], Mazlina Binti Abdul Majid [b,d],

[a] Department of Mechanical Engineering, UniversitiTeknologi PETRONAS, Perak, Malaysia
[b]Business School, Taylors University, Malaysia
[c] School of Materials and Mineral Resources Engineering, Universiti Sains Malaysia, Malaysia
[d]International College of Automobil, Pahang, Malaysia
[e] Nano-Optoelectronic Research (NOR) Lab, School of Physics, UniversitiSains Malaysia, Malaysia

* Corresponding author. Tel.: 0060 - 165505065;
E-mail address: PCC13011@stdmail.ump.edu.my

A b s t r a c t

Keywords:

Cloud security,
Cloud attacks,
DoS attack.

Distributed computing is a widely utilized approach for rapidly enhancing an organization's information technology capabilities while minimizing additional resource requirements. It can efficiently and effectively broaden an organization's existing IT competencies. In recent years, distributed computing has developed from being a novel and unfamiliar business idea into a rapidly expanding IT business sector. However, as additional organizations and individuals relocate their data and applications into the cloud, significant concerns are starting to develop regarding the infrastructure's ability to protect sensitive data. Despite the considerable movement toward cloud-based computing, venture clients remain hesitant to relocate their business data into the cloud. Security has proved to be a significant issue, and those concerns continue to diminish the development of distributed computing.

Accepted: 20 April2015

1. Introduction

As originally designed, the Internet was intended to facilitate straightforward data transfers between different interconnected workstations and systems. It was not designed to optimize data security[1]. However, the computerized equivalents of infections, pathogens, and other similar dangers have been observed since the origins of the Internet. In 1988, when the Internet's forerunner, ARPANET, was comprised of approximately 60,000 interconnected machines, a self-replicating PC system, the Morris Worm, unintentionally disabled nearly 10% of these machines.

Despite constant warnings, numerous organizations and individuals still fail to legitimately protect their computing resources. With a current user base in excess of 1 billion clients, the Internet has evolved into the preferred method for organizations and individuals to reliably and conveniently manage financial accounts, purchase retail products, access online classes, perform hotel and airline reservations, and numerous other tasks. Additionally, the rapid ascent of online social networking has greatly increased the Internet's

significance as a marketing platform, which has enhanced targeted marketing opportunities and created critical income sources[2] .

The disadvantage of this capability and convenience is vulnerability to intentional disturbances. Malevolent users frequently attempt to obtain sensitive data or disable typical workstation functions. Malevolent intentions frequently involve the theft of personal or financial data [3]. A digital attack by a pernicious gathering mechanism, intended to disturb a site on the Internet (or any mechanism joined with it), is termed an availability based attack. These attacks utilize a broad range of distinctive attack vectors, including TCP surges, Http and Https surges, low-rate attacks, SSL attacks, and others. As a result, availability based strikes are among the most significant security dangers affecting Internet sites.

These attacks are generally referred to as denial-of-service (DoS) attacks[4]. If the attack is executed by multiple machines, it is referred to as a distributed denial-of-service (DDoS) attack. DoS and DDoS attacks are widely reported in the news media, with articles describing how malignant hackers were able to cause critical downtime or rupture security for a well-known and trusted site.

2. Cloud computing overview

A. Software as a Service(SaaS)

Software-as-a-Service (SaaS) is a software deployment model in-demand licensing and utilization relieves the customer of the burden of installing, updating, and maintaining applications [5].

SaaS is typically billed based on the service's utilization frequency; thus, the quantity of resources consumed (and therefore the cost) typically reflects the level of activity. Driven by the IT industry's migration toward SaaS, in which software is not purchased but rented as a service from providers.

B. Platform as a service

IT users who require large platform at a low price should consider using platform as a service, PaaS[6]. Platform as a service also known as PaaS is also referred to as 'cloud ware'. It offers services such as; workflow facilities for application design, testing, application development, hosting and finally deployment.

C. Infrastructure as a service

This service simply offers the delivery of computer infrastructure, mostly in the form of platform virtualization environment. A good example of everything as a service trend and share common characteristics with other services is the 'virtual infrastructure stacks'. Clients purchase these services over the web instead of buying servers, data center space, network equipment's or software[7] .

D. IT as a service

This model incorporates venture portfolio, workflow reengineering, administration and procedure change[8].

A few years can be taken so as to finish the conversion of the ItaaS model. In order to help this conversion, many huge IT associations have received the Information Technology Infrastructure Library in short known as the ITIL. Through associations it is easier to; power their help work areas, evade downtime arising due to unapproved changes and they can convey enhanced administration to their clients by embracing best practices for overseeing the administration, IT possessions and progressions.

2.1. Cloud DoS and DDoS review

Different virtual machine; a good example being the virtualized servers are combined with the physical server's zone unit in the cloud setting.

Data focus security gatherings will not singularly duplicate average security controls for the insight focus in order to secure the virtual machines. They do these so as to boot exhortation their clients on approaches of using these machines to relocate on a cloud setting once applicable. The security software loaded onto a virtual machine must include a bidirectional stately firewall so as to enable the centralized management of a server firewall policy. This bidirectional stately firewall ignores solutions to; accessibility vulnerabilities including shutting down unused services, reducing users' permission, installing updated patches and the access rights to application.

Raj et.al [9] suggests resource should be isolated so as to facilitate data security during processing. Through isolating the resources the processor caches in virtual machine hence isolating virtual caches from the hypervisor cache. However, it is impossible to tell if cloud providers have correctly deleted a client's data or saved it. On the other hand, Basta and Halton suggest the use of encrypted protocols so as to prevent IP spoofing[10]. They further state that in order to avoid ARP poisoning one has to require root access to change ARP tables by; using static rather than dynamic ARP tables or ensure changes to the ARP tables are logged at a minimum.

The following is an example of presenting an intriguing view point: awkward questions about control and ownership arise due to allowing a third party services to take custody of personal documents. The questions awkward questions that arise are; "can you take data with you if you move to a competing service provider?" or "could you lose access to documents if you fail to pay a bill?" The issues of privacy and control cannot be eliminated completely but they are merely mitigated by using stringent service level agreements (SLAs) or designating the cloud itself to be private. One straight forward solution is utilizing in house "private clouds" .This solution is widely used for UK businesses. However, it has described a private cloud installation in their presentation, 'The Eucalyptus Open-Source Cloud-Computing System'.

When examining survival strategies for DoS and DDoS attacks one should include; understanding the fundamentals of attacks, distinguish characteristics from one another and methods employed to initiate them. The following scenario will provide an allegorical illustration of a DoS strike: a bank has only one open teller window, an individual with no bank related transaction intentions begins conversation with the teller. A client of the bank will be unable to make a transaction due to the 'noxious' client. The legitimate client will have to wait till the 'noxious' client has finished his discussion with the teller. This client eventually leaves but another one comes into the bank going straight front of the line in front of the legitimate client. This compels the legitimate client to continue waiting. This can go on for minutes, hours or even days preventing any legitimate clients from performing bank transactions. Throughout DoS attacks, the attackers foist excessive amounts of data upon a system hence debilitating the system and preventing clients from gaining admittance. DoS can simply be seen as the point which an attacker utilizes a machine to disable another machine, preventing it from working correctly[11] as shown in figure 1.

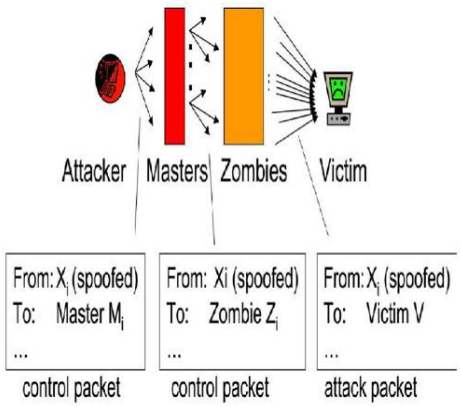

Fig. 1: The amplifying network in "direct DDoS attacks"

Commercial web servers are powerful to withstand a DoS attack from one machine, for example in the scenario above if the bank had more teller windows available to provide the legitimate client with other options apart from the occupied teller window. However, attackers regularly execute DDoS attacks which use different machines in order to expand the attack capacity[12]. In the scenario above, the added capacity due to availability of more teller windows can block the additional teller windows with non-legitimate users, hence, preventing legitimate users from completing bank transactions. In this scenario it is almost impossible to physically identify attackers. Innovative protections are used to identify and shield against this type of attack. Corrupting large numbers of work stations with malware so as to increase unapproved access to attacked machine, this is done by attackers so as to increase the scale of attack.

In the previous situation, which is the most common attack situation, it was seen that attackers create malware from various illicit vendors which is then spread to defenseless workstations. Clients are deceived into running the malware [13].

Hence, disabling anti-virus programs in their work stations, this creates an access point for attackers. Therefore, contaminated workstations start to act on commands from 'command and control' shortly known as C&C. These are machines which are coordinated mainly to send commands to botnet machines; they employ the Internet Relay Chat (IRC) protocol intended for chat rooms. When attackers decide to launch a DDoS attack, they simply send a message to their botnet's C&C servers with instructions to attack a specific target, the contaminated botnet machines controlled by the C&C servers will directly initiate the attack. Law enforcement technicians in attempt to disassemble a botnet must identify and disable the corrupted C&C servers, when these measures are completed they prevent most botnets from remaining operational.

In 2010 a botnet referred to as 'Mariposa' ,which is Spanish for butterfly was discovered and disable, the botnet contained approximately 15.5 million IP addresses from around the world with many cooperating command and control servers[14]. Some sophisticated botnet configuration an example the TDL-4 have advanced botnet correspondence capabilities over open distributed systems, hence, they are resistant to efforts to destroy the bonnets via the disabling of C&C servers. Programmers attempting to implement an attack may distribute text messages to similarly minded people by using an informal communication site or an IRC channel; this includes a date and time, instructions for utilizing available attack apparatus and target IP or URL. Hacking groups have applied this method and have successes in enrolling numerous supporters.

Cloud Malware Injection Attack, in this attack the attackers attempt to apply malicious service or code[15]. This appears to be a valid instance of services executing in the cloud. If the attacker is successful the cloud service is subjected to illicit monitoring. In this attack the attacker uploads a

corrupted copy of a victim's service instance. Hence, the service request to the corrupted service may be processed by malicious instance.

Distributed Denial of Service Attack shortly known as DDoS is a particular type of DoS attack where multiple compromised systems is utilized, which is infected with a Trojan horse. These systems are utilized to target a single system causing a Denial of Service (DoS) attack. As shown in figure 2, victims of DDoS attack include the targeted system and all systems maliciously utilized and controlled by the hacker in the distributed attack. DDoS attacks on cloud service are increasing.

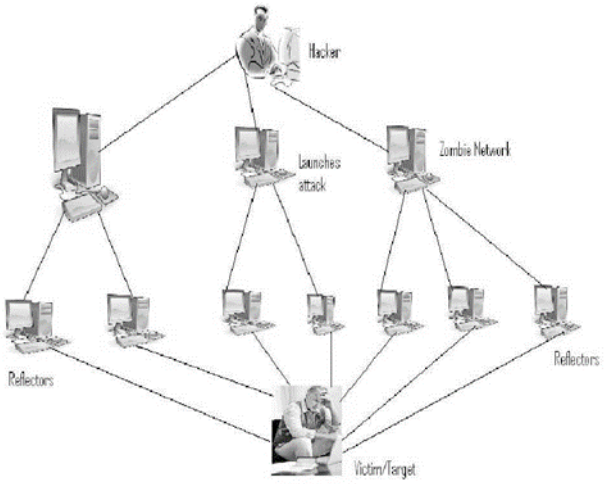

Fig.2: Distributed DoS Attack

Man-in-the middle attack also termed as fire brigade attack. It occurs when an attacker positions himself in the communications path between two users. This makes it possible for the attacker to intercept and temper with the data from those communications[16] .

Wrapping attack, attacks on cloud computing installations are becoming more serious due to increase in number and severity, this endangers the security and privacy of users worldwide [17]. Due to this industries have found the need to increase efforts to enhance cloud security. Cloud security researchers are attempting to measure the impacts of many security threats by using a framework or metric based on service level agreements since measuring threats to cloud security have proven to be difficult. Researchers have proposed a framework for designing a metric for specific environments. In the other hand scientist have proposed a service level agreement- based metric , which shown in figure 3.

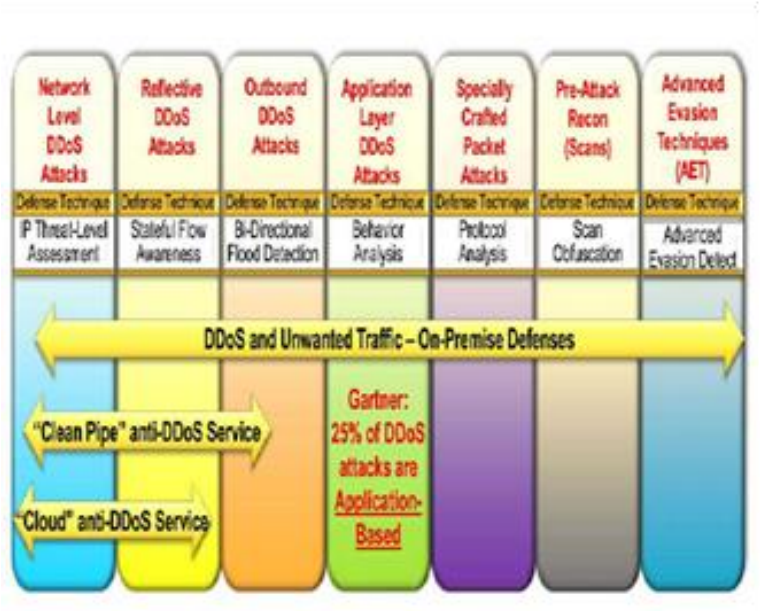

Fig.3: DDoS and Unwanted Traffic

4. Conclusions

In conclusion this paper has described the most current issues on DoS and DDoS attacks on cloud computing. Although, the idea behind cloud attack is to gain as much information that can be used in cloud computing, in some cases reducing the IT cloud resource. The question of the best method or hypothesis of mitigating thesis attack arises. A good answer to this question will be deep scholar security research for predicting these attacks before it happens in actual time.

References

[1] C. Natarajan, Improving Service Performance in Cloud Computing with Network Memory Virtualization, Recent Advances in Information and Communication Technology, Springer, 2014, 233-243.

[2] A. Alzahrani, N. Alalwan, and M. Sarrab, Mobile cloud computing: advantage, disadvantage and open challenge, 21.

[3] N. J. King, and V. Raja, "What Do They Really Know About Me in the Cloud? A Comparative Law Perspective on Protecting Privacy and Security of Sensitive Consumer Data, American Business Law Journal, 2013; 50(2): 413-482.

[4] A. Bakshi, and B. Yogesh, Securing cloud from ddos attacks using intrusion detection system in virtual machine. 260-264.

[5] S. V. YECHURI, and H. S. GOVADA, "SOFTWARE AS A SERVICE (SaaS), 2014.

[6] A. Gomes, "CLOUD COMPUTING: PLATFORM AS A SERVICE, 2014.

[7] A. K. Kar, and A. Rakshit, Pricing of Cloud IaaS Based on Feature Prioritization-A Value Based Approach, Recent Advances in Intelligent Informatics, Springer, 2014; 321-330.

[8] P. Mell, and T. Grance, "The NIST definition of cloud computing, 2011.

[9] H. Raj, R. Nathuji, A. Singh, and P. England, "Resource management for isolation enhanced cloud services. 77-84.

[10] A. Basta, and W. Halton, Computer security and penetration testing: Delmar Learning, 2007.

[11] T. Hirofuchi, H. Ogawa, H. Nakada, S. Itoh, and S. Sekiguchi, A live storage migration mechanism over wan for relocatable virtual machine services on clouds. 460-465.

[12] A. Chonka, Y. Xiang, W. Zhou, and A. Bonti, "Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks," Journal of Network and Computer Applications, 2011; 34(4): 1097-1107.

[13] S. Biggs, and S. Vidalis, Cloud computing: The impact on digital forensic investigations. 1-6.

[14] A. Schmidt, "Hierarchies in Networks: Emerging Hybrids of Networks and Hierarchies for Producing Internet Security," Cyberspace and International Relations, Springer, 2014; 181-202.

[15] S. Shafieian, M. Zulkernine, and A. Haque, Attacks in Public Clouds: Can They Hinder the Rise of the Cloud? Cloud Computing, Springer, 2014; 3-22.

[16] J.-M. Kim, and J.-K. Moon, Approach of Secure Authentication System for Hybrid Cloud Service, Advanced in Computer Science and its Applications, Springer, 2014; 1377-1384.

[17] H. Mahajan, and N. Giri, Threats to Cloud Computing Security.