Securing cloud computing environment by mitigating DDoS attacks: Moving target defence approach.

Kesavamoorthy R[1]*, Thangamariappan L[2], Ruba Soundar K[3]

[1]Kalaivani College of Technology, Palathurai, Madukkarai, Coimbatore, India
[2]Sree Sowdambika College of Engineering, Coimbatore, Tamil Nadu, India
[3]P.S.R. Engineering College, Coimbatore, Tamil Nadu, India

Abstract

Cloud computing with its recent development, made it's accessible by almost everyone. Millions and millions of people daily store their data in the cloud platform and utilize for various kind of need. In this scenario, distributed denial of service (DDoS) attacks is one of the common issues in the day-to-day usage, which severally affects the availability of the resources or services. The challenge is to create a DDoS detection and mitigation system that can protect against both volumetric and application-specific resource starvation and exhaustion attacks. In this paper, a new method named MOTAG has been proposed. This method of moving-target defence to overcome DDoS attacks will repeatedly shuffle the assignments between client to server in order to identify the malicious clients first and then to quarantine them.

Keywords: Cloud computing, DDoS, Detection, Mitigation, Malicious.

Accepted on January 06, 2017

Introduction

Considering the three major threats in cloud computing, confidentiality, integrity and availability, the latter one plays the primary role in many businesses' success. Various recent surveys indicate that web based businesses alike prefer systems that operate reliably to those that offer greater security but at the expense of more service interruptions [1]. Frequent disruptions can directly impact any organization in terms of their profit, productivity, and reputation of course may be the first.

Almost all the web based businesses employ redundant hardware and service replicas in order to increase the availability of their services. However, in contrary to a conservative design principle [2], systems are frequently engineered and tested under normal rather than worst-case conditions. Consequently, they are vulnerable to attacks that cause either resource exhaustion or resource starvation, but ultimately resulting in a partial or complete denial of service (DoS) to the legitimate users.

Impact of distributed computing on DoS attacks

To improve the performance and efficiency, the introduction of distributed computing made the components of a software system to be shared among multiple computers in various geographic locations. On the other hand, this same impact of distributed computing shifted the target of DoS or DDoS attacks from small groups of isolated machines to the integrated computer networks of various types of large-scale enterprises. An early example of this phenomenon occurred in when 10-year-old Michael "Mafiaboy" Calce, motivated simply by a desire for unsavory reputation resulted in the shutdown of several major websites, including Amazon, CNN, eBay, and Yahoo (then the world's largest search engine) within hours of launching a DoS attack [3].

Current DDoS trends make it clear that yesterday's strategy is no longer defensible. New and more sophisticated DDoS varieties are emerging, requiring organizations to be both highly flexible and ready for anything that might come their way. In 2012-2013, for example, a series of DoS attacks dubbed Operation Ababil and launched by the self-proclaimed "Izz ad-Din al-Qassam Cyber Fighters" targeted several major US financial institutions and was both politically and religiously motivated, Schwartz 2013.

Nowadays, most DoS attacks are implemented as distributed DoS (DDoS) attacks. These use thousands to millions of computers distributed across the internet to attack a target, making it difficult to identify and block the attacker.

Literature review

Various defences have been employed to prevent or mitigate the impact of DDoS attacks, including

- Filtering based approaches that use ubiquitously deployed filters to block unwanted traffic sent to the protected nodes [3-5]
- Capability based mechanisms that constrain a user's resource utilization to beneath a threshold defined by the defended system [6-9] and
- Secure overlay solutions that interpose a network of server nodes that redirect packets between clients and the protected nodes and are designed to absorb and filter out attack traffic [10-12,6].
- All these defences are effective to some degree but are static and rely on the global deployment of additional functionalities on internet routers or large, robust, virtual networks designed to withstand ever-larger attacks. Moreover, they require large investment to implement and are vulnerable to sophisticated attacks, such as sweeping and adaptive flooding [10]. Thus, developing novel, effective, efficient, and low-cost DDoS defences is a high priority.

Better security against stronger attacks

As security has increased at the network and transport layers, attackers have moved up the protocol stack. The security community is very familiar with volumetric DDoS attacks at the network and transplant layers but less so with DDoS attacks at the application layer, which have been on the rise since 2010 and pose an additional threat that can't be ignored [13].

According to Common Weakness Enumeration 400, (https://cwe.mitre.org/data/definitions/400.html), a system is exposed to resource exhaustion and starvation if it fails to properly restrict the amount of resources that are used or influenced by an actor. This includes, but isn't limited to, infrastructure resources, such as bandwidth and connection pools, and computational resources, such as memory and CPU time. These attacks typically occur at the network and transport layers, Wang 2014, but the asymmetric nature of communication protocols, design and coding errors, and inherently expensive tasks all contribute to applications' susceptibility to such attacks [13].

The challenge is to create DDoS detection and mitigation system that's agnostic of the underlying service and thus can protect against both volumetric and application specific resource starvation and exhaustion attacks.

MOTAG: A cloud-based moving target defence

With this challenge in mind, researchers at George Mason University's centre for assurance research and engineering (CARE), created a defensive mechanism against DDoS attacks that leverages the redundancy most modern systems exhibit in terms of network presence and computational capacity [12]. We relied on the prevalence of data centre and cloud services to develop MOTAG, a moving-target defence mechanism that segregates benign from malicious requests and can operate effectively even in the case of new or previously unseen attacks.

Our approach rests on four key assumptions:

- Malicious clients can easily blend with benign ones and thus can't be separated on the basis of location, request content, or request volume;
- An attack can be detected through increased use of resources or service non-responsiveness, but the individual attacker can't be easily identified;
- We control the mapping between protected servers and incoming clients (either benign or malicious) and can reassign clients to different servers on demand; and
- We can reassign clients from one server to another without significant loss of resources or user-perceived server downtime.

To set up MOTAG, we reserve computing capacity and network bandwidth to meet the needs of the servers used in normal operations as well as provide sufficient capacity to instantiate a small number of additional server nodes in the event of a DDoS attack. Each server node is identical, and all can handle user requests independently.

The instantiated server nodes can be divided into two groups. The first one is relatively static serving server nodes that provide more reliable services in terms of connection for known innocent clients. The second one is dynamic shuffling server nodes that will shuffle (reassign) operations to provide blinking or discontinuous connections to suspicious clients. During a DDoS attack, MOTAG will replace the shuffling server nodes with new ones and reassign the associated clients to those new nodes. This shuffling of clients presents a continually moving target for the attacker and makes it possible to isolate malicious clients.

In this simple example in Figure 1, the protected system has two servers for normal operations, and each is under attack by a malicious client blended with innocent clients (C1-C4). MOTAG instantiates two additional servers and repeatedly shuffles, or reassigns, the clients to the new servers until only one is under attack, making it possible to identify and segregate the attackers. In real-world cases, the shuffling process usually requires multiple rounds and involves multiple clients and servers.

On the move

Prior to a DDoS attack, all active server nodes are untagged and MOTAG randomly assigns each client to only one of them. MOTAG tags server nodes that subsequently come under attack as shuffling server nodes; the nodes that remain untagged constitute serving server nodes. Once a server node or nodes come under attack, MOTAG repeatedly shuffles the client-to-server assignments within the shuffling server group to distinguish, and eventually segregate, attacking clients

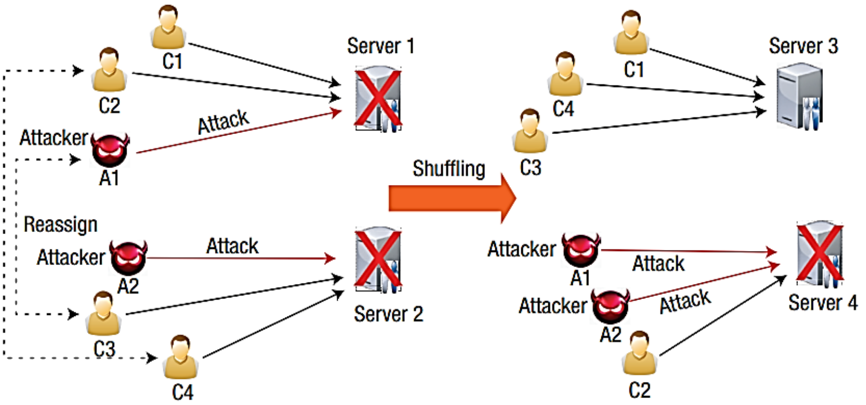

Figure 1. *MOTAG defence against DDoS attacks.*

from innocent ones. Figure 1 is a simplified illustration of this process.

During the process of every shuffle, the shuffling server nodes with malicious clients will still be vulnerable to attack because those clients know the nodes' location obviously through IP address. Those shuffling server nodes that are in the safer state will become serving server nodes hereafter, and MOTAG will tag the associated clients as trusted and consider them safe from the ongoing attack.

MOTAG considers clients connected to the attacked server nodes untrusted as it can't determine which clients are attackers. To isolate innocent clients, it randomly redistributes all untrusted clients across the shuffling server nodes. Given an estimated number of suspicious clients and the available server nodes, MOTAG can instantiate new server nodes as shuffling server nodes to accelerate the isolation of malicious clients from innocent ones.

Optimization

The greater the number of nodes MOTAG uses as shuffling servers, the faster it will quarantine malicious clients and insulate innocent ones. By repeating the client-to-server shuffling for multiple rounds, it can gradually identify most of the innocent clients. Based on the estimated number of attackers and given a desired percentage of clients to be saved, it initiates a limited number of shuffling rounds after which the expected percentage of innocent clients will be insulated, the remaining clients quarantined, and the attack damage minimized.

To reduce overhead, the shuffling process is stateless, meaning that each shuffle is considered independent. MOTAG resets the trusted/untrusted tags it has placed on clients after each shuffle. These tags don't necessarily reflect the clients' true identity, but instead characterize the server node to which they're assigned.

In addition, the shuffling and serving roles of server nodes are interchangeable across shuffles, depending on attacker behaviour-for example, previously untagged server nodes can become shuffling server nodes if attacked during the shuffling process. The goal of MOTAG's shuffling operations is to separate innocent but attacked clients from truly malicious clients to preserve the system's availability for innocent clients.

Additional Discussion

Scientists examine cloud computing as a cost-effective and energy-efficient computing paradigm to accelerate discoveries in biology, climate change and physics. The introduction of the Science Clouds project allows members of the scientific community to lease resources for short amount of time. Such kind of cloud environment faces significant threat from the DDoS. Keeping this in mind, this paper presented a novel method to overcome DDoS attacks in which the attack detection and recovery time is minimal. This is one among the milestone in retaining the availability services of cloud computing and thereby contributed a little bit towards the objectives of scientific community.

Conclusion

Our paper started with introduction to the impact of DDoS, it analyzed various works related to mitigating DoS and DDoS attacks. The proposed moving-target defence divided the server nodes into static serving server nodes and dynamic shuffling server nodes. The key idea is that, this mechanism repeatedly shuffles the assignments between client to server in order to identify the malicious clients. This method not only insulates the innocent clients from DDoS attacks but also quarantines the identified malicious clients over time. Even during the time of attack, the protected system will be available to most innocent clients and thereby protecting the organization's reputation, productivity, and revenue. Since, MOTAG identifies malicious users solely by detecting if the server is under attack, attackers can't escape detection by acting like normal users.

References

1. Gruman G. Mobile users favour productivity over security: As they should. InfoWorld. 2014 [www.infoworld.com/article/2686762/security/mobile-users favour productivity-over-security-as-they-should.html]. Accessed on: September 26, 2014.
2. Saltzer JH, Schroeder MD. The protection of information in computer systems. Proc. IEEE. 1975;63(9):1278-08.
3. Ferguson P, Senie D. Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing IETF RFC 2827 May 2000.
4. Schwartz MJ. Bank attackers restart operation Ababil DDoS disruptions dark reading. 2013 [www.darkreading.com/attacks-and-breaches/bank-attackers-restart-operation-ababil-ddos-disruptions /d/d-id/1108955]. Accessed on: March 6, 2013.
5. Liu X, Yang X, Lu Y. To filter or to authorize: Network-layer DoS defense against multimillion-node Botnets. Proc. ACM SIGCOMM Conf. (SIGCOMM 08) 2008;13:195-206.
6. Mahimkar A, Dange J, Shmatikov V, et al. dFence: Transparent network-based denial of service mitigation Proc. 4th USE-NIX Symp. Networked systems design and implementation (NSDI 07) 2007.
7. Anderson T, Roscoe T, Wetherall D. Preventing internet DoS with capabilities. ACM SIGCOMM computer communication rev. 2004;34(1):39-44.
8. Liu X, Yang X, Xia Y. Net-fence: Preventing internet denial of service from inside out. *Proc.* ACM SIGCOMM Conf. (SIGCOMM 10) 2010;255-66.
9. Yaar A, Perrig A, Song D. SIFF: Stateless internet flow filter to mitigate DDoS flooding attacks, Proc. IEEE symp. *Security privacy* (S&P 04). 2004;130-43.
10. Andersen DG. Mayday: Distributed filtering for internet services *Proc. 4th USENIX Symp. Internet Technol Sys* (USITS 03). 2003;4.
11. Dixon C, Anderson T, Krishnamurthy A. Phalanx: Withstanding multimillion-node Botnets, Proc. 5th USENIX Symp. Networked systems design and implementation (NSDI 08). 2008;45-58.

12. Jia Q, Sun K, Stavrou A. MOTAG: Moving target defense against internet denial of service attacks, Proc. 22nd International Conf. Computer communications and networks (ICCCN 13). 2013.
13. Mantas G, Stakhanova N, Gonzalez H, et al. Application-layer denial of service attacks: Taxonomy and Survey. Int'l J information and computer security. 2015;7(2-4):216-39.

***Correspondence to:**

Kesavamoorthy R
Department of CSE
Kalaivani College of Technology
Coimbatore-641105
Tamilnadu
India
Tel: +91 8526886313, 04222621000
E-mail: kesavamoorthycse@gmail.com