X-DoS (XML Denial of Service) Attack Strategy on Cloud Computing

Shruthi B T1, Dr.Y.S.Nijagunarya2
1Mtech student, Dept of CSE, Siddaganaga Institute of Technology, Tumkur, India.  
2Professor, Dept of CSE, Siddaganga Institute of Technology, Tumkur, India.

Abstract: Cloud computing is an emerging trend. It allows customers to obtain cloud resources and services. Cloud Computing is suffer from Denial of Service (DoS) and Distributed DoS/DDOS attack. The effects of DoS attacks mainly involve exhaustion of resources like memory, network bandwidth etc which affect the service availability and performance of the system. Attackers are aware of old DDoS protection mechanism. So, they try to do their activities in a “stealthy” fashion which is mainly specialized for X-DoS attack. Therefore, we should give concentration for stealthy DoS attack which may fools innocent victim s. Stealthy attack problem in cloud incurs poor QoS and high service maintenance cost in terms of resource consumption. A technique named Slowly Increasing Polymorphic DDoS Attack Strategy (SIPDAS) is proposed against Stealthy DoS attacks in which stealthy attack pattern are orchestrated to detect and eliminate it and also show the effect incurred on the target system. Cloud management system has to maintain certain host based countermeasures in order to avoid accidental or deliberate intrusion.

1. Introduction

Cloud computing is a type of computing that store, manage and deliver service over the Internet. Naturally, it prone to notorious DDoS attacks in a cloud environment. The main effect of DDoS is degrading Quality of Service (QoS), service availability, performance and high maintenance cost due to resource consumption is more. This DoS attack exhausts the resources like memory, network bandwidth and processing resources [1]. DDoS attack is more dangerous because it spread from one to many systems and may stop working of target server system as shown in Fig.1. It is very difficult to detect the degraded QoS which may be taken as issue of security vulnerability. Therefore, Cloud management system has to maintain certain host based countermeasures in order to avoid accidental or deliberate intrusion. Traditionally, there are several method has been used in order to detect DDoS attack like worst-case threshold, time-window, rate-controlling and pattern-matching methods in order to differentiate malicious behavior from legitimate one[2]. However, attackers are aware of old DDoS detection mechanism. So, they try to do their work in a “stealthy” manner which is mainly specialized for X-DoS attack in order to degrade specific target system [3].

This paper proposed a new technique in order to compose stealthy attack patterns namely SIPDAS (Slowly-Increasing-Polymorphic DoS Attack Strategy) against application running on cloud. The proposed strategy aims at exhausting cloud resources and cloud flexibility. It is an iterative & incremental approach. The proposed strategy is specialized for X-DoS attack. In X-DoS attack XML tag is injected into SOAP message in order to modify the XML data structure. This is mainly by SIPDAS core algorithm. The target system degraded can be checked by using approach count-and-threshold mechanism. Attack achieved successful or not can be measured by using technique chebyshevs inequality theorem. The features of cloud provider like load balancing and auto scaling can also be maliciously exploited by proposed strategy. Using SIPDAS induces overload on target system in order to delay the detection mechanism. We mainly focus on serious threat like XML-based DoS attack. We implement this using Amazon S3 which offers both features like auto scaling and load balancing.

2. Background And Related Work
2.1 Related Work

Sophisticated DDoS attack is a type of attacks, which degrade the target system in order to do DoS attack or degrade the performance or exhaustion of resources [4], [5]. The term stealthy means without knowing to user doing attack secretly [6]. This is a attack which is done invisibly for the detection mechanism by the attacker. This stealthy attack is very difficult to detect when compared to old flooding style and brute force attacks [7]. Sophisticated attacks are done by sending a low rate traffic which is unrecognized by DDoS detection mechanism. In recent days, more DoS attack variants uses low rate traffic such as LDoS( shrew attack), RoQ (Reduction of Quality attack) and LoRDAS (Low-Rate DoS attacks against application servers). There is a high similarity of this low rate traffic to legitimate network traffic. This new type of attack cannot be powerfully prevented or detected. They presume the target server has finite queue. Each service request will be stored in the queue. So, the attacked server is busy in processing malicious request than the legitimate user request. It is very difficult for target server to differentiate which is malicious request and legitimate request users.

2.2 Cloud Resource Provider

Cloud service providers offer services to rent storage capacity giving ‘unlimited resource availability’. They allow customers to fetch and configure system capacity. It also offer features like ‘load balancing’ and ‘auto scaling’ (adds or remove instances). The proposed work shows how the features of cloud provider are maliciously exploited in order to degrade the target system. Fig.2. shows the cloud resource provisioning.

2.3 The Amazon S3

Amazon S3 (Simple Storage Service) is a cloud service provider which offer facility of online file storage services provided by Amazon. Amazon uses the same scalable storage infrastructure. Amazon S3 provides high availability, scalability and low latency. Amazon S3 allows enable or disable user logging. The user log has information like HTTP Status, turnaround time (tat), Protocol used and Access Date / time etc. These logs are managed and analyzed by using third-party tools such as S3Stat, AWS Stats, Splunk, Qloudstat or Cloudlytics[10]. It has cloud feature like auto scaling and load balancing which is very user friendly.

Fig.3. Amazon S3

3. DoS Attack Against Cloud Application

DDoS attacks which exhaust the resources of cloud application is the severe security vulnerabilities. [8], [5], [9], [11]. Its effect include high memory usage, degrade target server system, Oversize Payload attack, XML tag injection into a SOAP to modify the XML data structure, degrade QoS. The Deeply-Nested XML is type of attack which exhausts the resources by injecting large number of nested tags into XML message format which parses the XML analyzer in the application server. [9].

4. Stealthy DoS Characterization And Modeling

It gives features for DDoS attack to be stealthy on cloud application.

- If the system is under DDoS attack then system performance is more degraded.
- The service time to process stealthy user request is more than the normal user.
- Processing of malicious request yields more resource consumption.
- Attack potency is more (i.e. ratio of damage caused by attacker/resource consumption)
4.1. Server Under Attack Model (SUA)

Fig. 4. shows an attack scenario of the system under attack model which is used to make service degradation. System consists of a pool of distributed VMs. There are $n$ legitimate service requests and $w$ is the cost to process the cloud resources. System consists of a queue of load balancing which has both legitimate requests and DDoS attack user requests. Each job of service request is processed by the system.

4.2. Stealthy Attack Objective

The main objective is to make attack pattern to be stealth. In order to do this we degrade the service request in term of aspect namely attack profit ($P_a$) and resource consumption ($C_a$). Stealthy DDoS is successful in cloud if function profit and resource consumption is more. When,

$$ P_a = \sum_{j=1}^{n} g(\phi_j), $$

$$ C_a = \sum_{j=1}^{n} w(\theta_j), $$

4.3. Creating Service Degradation

To exhaust the target resources, a number $n$ of flows $\phi(A_j)$ have to be orchestrated, such that:

$$ C_0(t_0) + C_n(T) + C_a(T) \geq C_m * T $$

Where $C_a(t)$ represents malicious request process load during the period ‘$t$’. The term $C_n$ can be neglected during the attack ($C_a >> C_n$), the malicious resource consumption $C_a$ can be maximized if the following condition is verified:

$$ C_a(T) \geq C_m * T - C_0(t_0) \text{ with } C_a >> C_n $$

5. Proposed SIPDAS Against Cloud Application

It describes the strategy to implement attack pattern which maximize profit and resource consumption. We propose SIPDAS (slowly increasing polymorphic attack strategy) which is iterative and incremental approach.

5.1 Attack approach

SIPDAS has three main components:

- Master - coordinate attack
- Agent - inject single flow of message
- Meter - evaluate attack

Algorithm 1 describes the implementation. It has agent which will inject a flow of messages in order to do stealthy service degradation against cloud application. This algorithm is mainly specialized for X-DoS. XML tag will be injected into a SOAP message. Initially, number of nested tag is taken as 0 i.e $N_t=0$. Maximum number of nested tag is injected in order to modify the XML data structure. Added nested tag is compared with initial tag in order to detect X-DoS attack. Tag injection is an iterative and incremental approach. Meter evaluates the Status of attack using Chebyshev’s inequality theorem. It uses probability distribution of $1/k^2$. It uses standard mean deviation. It takes sample of above upper bound of standard deviation as attack successful and rest as unsuccessful.

Target server degradation can be checked by using count-and-threshold mechanism. It is done based on threshold values. If it exceeds certain threshold then the service degraded. It has condition as follows using filtering function:

$$ y(0) = 0; $$

$$ y(i) = y(i-1) + 1 \text{ if } t_0(\phi_i) > c(\theta_i); $$

$$ y(i) = y(i-1) + D \text{ if } t_0(\phi_i) \leq c(\theta_i); $$

with $D \in [0,1]$ and $\phi_i \in \theta_k$.

Architecture consists of two independent application ‘Attacker’ and target server system namely ‘SUA’. Both set run on independent VM’s. SUA is XML-based web application: it receives XML messages via HTTPgw cloudlet which manages HTTP messages and forwards them to XML Analyzer, which perform XML parsing, and store result in Key Value store. Whenever virtual node is overloaded it automatically scales up by starting new VMs. We will evaluate each virtual machine resource consumption and number of retrieved message processed. Architecture is shown in Fig. 5.
The detail implementation of attacker is shown in Fig.6. SIPDAS attack can be done by as a service through simple web application.

Fig.5. Architecture

Attacker implementation is done in terms of cloudlet. Whenever web interface is attacked, parameter will be sent to Master.

Fig.6. Attack implementation

The Master will coordinate the attack. Agent will inject a flow of messages & the Meter will evaluate the attack effect. The KV Store is shared among all these Cloudlets which maintain the attack state information. The Master will fetch information from the KV Store and send message to Agent in order to update their action.

6. Experimental Result

In the experiment, we have done SIPDAS attack namely X-DOS (XML based DoS attack). We analyze the effect of X-Dos effect on cloud system. The attack effect consist of two independent applications namely ‘attacker’ and ‘SUA’ run on different VM’s. The SUA is a web application which receives XML tags injected into SOAP message and do XML parsing which modify the XML data structure and stores the result in Key-Value store. Then, the user can efficiently detect the X-DoS attack and block the malicious service request. Hence, the time consumption for processing job is less. Bar graph in the figure 7 shows number of user is in Waiting
State, Active State and X-DoS Attacked State in the web application.

![Fig.7. X-DoS Attack Graph](image)

7. Conclusion

In the present days, internet applications are always suffer from security vulnerability. Cloud computing is a part of internet based computing which is prone to harmful DDoS attack. We propose a strategy against stealthy attack pattern namely SIPDAS which orchestrate stealthy attack exploiting the target system. It also helps to detect the low rate traffic attack. The Proposed strategy aims at providing cloud flexibility, scales up the services and retains the QoS. The orchestrated sophisticated strategy can able to distinguish malicious service request from the legitimate service request.

8. References


