Web Services in DDoS Attack by Classify the Attacks

Suji .S[1], Chandraprabha .K[2]

[1]M.E, Computer Science and Engineering, K. S. Rangasamy College of Technology, Tiruchengode

Abstract: ***A website DDoS is executed by flooding one or more of the site's web servers with so many requests that it becomes unavailable for normal use. If an innocent user makes normal page requests during a DDoS attack, the requests may fail completely, or the pages may download so slowly as to make the website unusable. DDoS attacks typically take advantage of several computers which simultaneously launch hundreds of thousands of requests at the target website. The attackers are most likely going to use non-commercial computers as attack platforms, because they are usually easier to break.To solve the problems, several defense mechanisms against DDoS attacks have been proposed in the literature. However it is not easy for a security manager to select solutions suited for his service environments. Under the respect, this is intended to classify DDoS defense systems based on the functional design method. Also various experimental results of DDoS defense systems by using our proposed classification of defense systems and performance metrics.***

Keywords: Denial-of-service, Cloud computing, Mitigation, Web services, SOAP, XML, HTTP, Filtering

1. Introduction

A distributed denial-of-service is one of the main network or computer attack that provides a number of hosts to a webserver, a complete system crash by causing a website. The denial-of-service attack is to attack target large-scale, far-reaching, web services and popular websites by the hackers. This is targeted webserver with multiple requests, which disables the web services and prevents it operating system. The attacker recruits zombies by detecting multiple machines across the Internet, creating a botnet. These distributed botnets to multiply the strength of the attack malicious sources can be to filter out and hides the true identity of the attacker. The cloud computing and web services, even more dependency is put on the security and availability of resources accessible over the Internet.

2. Overview

2.1 DDoS attack

A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. They target a wide variety of important resources, from banks to news websites, and present a major challenge to making sure people can publish and access important information. DDoS protection, provisioned as a service at the network edge, matches the sophistication and scale of such threats, and can be used to mitigate DDoS attacks of all forms and sizes including those that target the UDP and ICMP protocols, as well as SYN/ACK, DNS amplification and Layer 7 attacks.

2.2 Web Service

A Web Service is a method of communication between two electronic devices over a network. It is a software function provided at a network address over the web with the service always on as in the concept of utility computing. A software system designed to support interoperable machine to machine interaction over a network

2.3 XML Attacks

XML attacks target web services that communicate through XML documents. SOAP mostly uses XML for passing data between the client and server. Attackers construct malformed XML requests and send these to the web service. Even a single malformed request might be extremely resource intensive to process. Hence, the attacker can cause considerable harm with a minimum amount of resources.XML attacks target web services that communicate through XML documents. SOAP in XML for passing data across the client and server. Attackers form the malformed XML requests and send across web service. An HTTP attack is requested attacker floods with non-specific HTTP requests in web services. As the web service is distributed denial of service attack to describe the multiple resource

2.4 HTTP Attacks

An HTTP attack is very rudimentary: the attacker floods a web service with non-specific HTTP requests. As the web service tries to process all requests and the particular service requires heavy use of resources, a denial-of-service is easily achieved

2.5 Genetic Algorithm Classifier

Genetic Algorithm to identify various harmful/attack type of connections. This algorithm takes into consideration of different features in network connections such as a type of protocol type, duration, service, dst_host_srv_count to generate a classification on rule set. Each rule set identifies a specific type of attacks.

An improvement on a classical technique, the k nearest neighbor’s algorithm, that believe shows a good deal of promise the improvement involves using an artificial intelligence technique, a genetic algorithm, to enhance the performance of the classical algorithm. The k nearest neighbor’s algorithm classifies a new instance by noting its distance from each member of a database of classified examples and assigning the new instance to the class of the majority of its nearest neighbors. This algorithm can be quite effective when the attributes of the data are equally important. The nearest neighbor classification algorithm (NN) is based on the idea that, given a data set of classified examples, an unclassified individual should belong to the same class as its nearest neighbor in the data set. The measurement of proximity, or similarity, between two individuals is a subject of much research although this is an important issue for classification.

2.6 Genetic Fitness Process

Genetic algorithms have two important features that underlie their success. The first is their employment of an algorithmic equivalent of natural selection. When chromosomes are chosen as parents during the reproduction process, the probability that a given chromosome will be chosen is biased in accord with its fitness. Thus, the fittest chromosomes (those that solve the problem best) will tend to have more children than the less fit ones. The use of fitness-based reproduction generally leads to an improvement in the population as a genetic algorithm runs.

Genetic algorithms (GAs) solve optimization problems by manipulating a population of chromosomes, encoded solutions to the problem. Each chromosome is assigned a fitness that is related to its success in solving the problem. Given an initial population of chromosomes, a genetic algorithm proceeds by choosing chromosomes to serve as parents and then replacing members of the current population with new chromosomes that are (possibly modified) copies of the parents.

3. Cloud Architecture

The common, unprotected cloud architecture contains the QQ following entities can be described

3.1 Cloud Providers

The providers are the actual workhorses of the cloud environment. The cloud dynamically deploys the virtual machines and web services on these entities.

3.2 Cloud Broker

The Cloud Broker listens to the initial request by the user. It keeps track of the available cloud providers and allocates the necessary resources for the user.

3.3 User

A user is a client that connects to the Cloud Broker to request resources from the cloud environment. Eventually, it can interact with the web services deployed in the Cloud Providers.

4 Algorithm

```
Input:
P ← Packet
S← Packet source IP address
D← Packet destination IP address
B← Blacklist
W←Whitelist
Begin:
If (S W && S∉B)
Forward P to D
Else If (S B) Drop p Else forward p to a V-node End
```

Step 1. Over-Provision Bandwidth to Absorb DDoS Bandwidth Peaks
This is one of the most common measures to alleviate DDoS attacks, but it is also probably the most expensive, especially since DDoS attacks can be ten times or even one hundred times greater than standard Internet traffic levels. An alternative to over-provisioning Internet bandwidth is to use a security service to scale on-demand to absorb and filter DDoS traffic. DDoS protection services are designed to stop massive DDoS attacks without burdening businesses' Internet connections.

Step 2. Monitor Application and Network Traffic The best way to detect when you are under an attack is by monitoring application and network traffic. Then, you can determine if poor application performance is due to service provider outages or a DDoS attack. Monitoring traffic also allows organizations to differentiate legitimate traffic from attacks. Ideally, security administrators should review traffic levels, application performance, anomalous behavior, protocol violations, and Web server error codes. Since DDoS attacks are almost always executed by botnets, application tools should be able to differentiate between standard user and bot traffic. Monitoring application and network traffic provide IT security administrator's instant visibility into DDoS attack status.

Step 3. Detect and Stop Malicious Users There are two primary methods to identify DDoS attack traffic: identify malicious users and identify malicious requests. For application DDoS traffic, often times identifying malicious users can be the most effective way to mitigate attacks.

1. Recognize known attack sources, such as malicious IP addresses that are actively attacking other sites, and identifying anonymous proxies and TOR networks. Known attack sources account for a large percentage of all DDoS attacks. Because malicious sources constantly change, organizations should have an up-to-date list of active attack sources.
2. Identify known bot agents; DDoS attacks are almost always performed by an automated client. Many of these client or bot agents have unique characteristics that differentiate them from regular Web browser agents. Tools that recognize bot agents can immediately stop many types of DDoS sources.
3. Perform validation tests to determine whether the Web visitor is a human or a bot. For example, if the visitor's browser can accept cookies, perform JavaScript calculations or understand HTTP redirects, then it is most likely a real browser and not a bot script.
4. Restrict access by geographic location. For some DDoS attacks, the majority of attack traffic may originate from one country or a specific region of the world. Blocking requests from undesirable countries can be a simple way to stop the vast majority of DDoS attack traffic.

Step 4. Detect and Stop Malicious Requests Because application DDoS attacks mimic regular Web application traffic, they can be difficult to detect through typical network DDoS techniques. However, using a combination of application-level controls and anomaly detection, organizations can identify and stop malicious traffic. Measures include:

1. Detect an excessive number of requests from a single source or user session—Automated attack sources almost always request Web pages more rapidly than standard users.
2. Prevent known network and application DDoS attacks—Many types of DDoS attacks rely on simple network techniques like fragmented packets, spoofing, or not completing TCP handshakes. More advanced attacks, typically application-level attacks, attempt to overwhelm server resources. These attacks can be detected through unusual user activity and known application attack signatures.
3. Distinguish the attributes, and the aftermath, of a malicious request. Some DDoS attacks can be detected through known attack patterns or signatures. In addition, the Web requests for many DDoS attacks do not conform to HTTP protocol standards. The Slowloris attack, for example, includes redundant HTTP headers. In addition, DDoS clients may request Web pages that do not exist. Attacks may also generate Web server errors or slow Web server response time

3.4Service-oriented Traceback Architecture

SOTA is a web security application that is product-neutral. Its main objective is to apply a SOA approach to Traceback methodology. This is in order to identify a forged message identity, since one of the main objectives of X-DoS and DX-Dos is to hide the attacker is true identity. The basis of SOTA is founded upon the deterministic **Packet Marking algorithm**.

Deterministic Packet Marking algorithm marks the ID field and reserved flag within the IP header. As each incoming packet enters the edge ingress router it is marked. The marked packet will remain unchanged as they traverse the network. Outgoing packets are ignored. DPM methodology is applied our SOTA framework, by placing and the Service Oriented Traceback Mark within service messages.

3.5 XML-Based Denial Of Service(X-DOS) Attacks

A denial of service is where attacks deprive legitimate users of their sources. An X-DoS is where a network is flood with XML message instead of packets in order to prevent legitimate users to access network communications. Further, if the attacker floods the web server with XML requests, it will affect the availability of these web services.

4. Conclusion

It not get the desired information effectively. The DDoS solves this problem and helps the users to fulfill their needs. Since filtering not affected by number of packets, the packets sent by legitimate customers will have the frequent correlation characteristics as usual. Thus these packets will also get a high CBF score to avoid being bloc ked. Cloud Traceback can be used in an actual X-DoS attack, so the cloud victim could trace the attack back to source. This results showed that CTB is able to find the source of an attack within a matter of seconds. Application-layer vulnerabilities impose an enormous risk for the availability of web services. The tested attacks have proven to clog up a web server with a minimum amount of attack resources. A distributed attack is not even necessary, as a single machine and even a single request have proven to successfully execute a denial-of-service attack. To mitigate this risk, a defense system is proposed and implemented. The system tests concluded that it is effective at detecting and mitigating these attacks. Besides, the defense system incorporates detection of all reported vulnerabilities and might be able to detect still unknown attacks because of its normal request model. However, if new attack techniques using other request semantics should arise, additional features have to be implemented. Finally, the response time overhead that is introduced is minimal. The system effectively is faster than the considered alternatives.

Reference

[1] Chonka, Singh, and Zhou,“ Chaos theory based detection against network mimicking DDoS attacks”, IEEE Commun. Lett. 2009, pp. 717–719.

[2] Chonka, Zhou and Xiang,“ Protecting web services from DDoS attacks by SOTA”, In: Proceedings of the IEEE fifth international conference on information technology and applications,IEEE,2008.

[3] Chonka,Zhou ,“ Defending grid web services from X-DoS Attacks bySOTA ”, In: Proceedings of the third IEEE international work shop on web and p ervasive security,IEEE,2009.

[4] Gulshan Shrivastava, Kavita Sharma, “The Detection &Defense of DoS&DDoSAttack:A Technical Overview” Proceeding of ICC, pp.27-28, December 2010.

[5] Kim, Lau, AND Chuah, H.J. Chao, “Packetscore: a statistics-based packet filtering scheme against distributed denial-of-service attacks”, IEEE Trans.Dependable Secure Comput. 3 (2) (2006) PP.141–155.

[6] Mahbub Ahmed, “Above the Trust and Security in Cloud Computing: A Notion towards Innovation”, IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, 2010.

[7] Peng, Leckie, and Ramamohanarao,” Survey of network-based defense mechanisms countering the DoS and DDoS problems”, ACM Comput. Surv. 39 2007.

[8] Xiang, Zhou, “Low-rate DDoS attacks detection and traceback by using new information metrics, IEEE Trans. Inf. Forensics Secur. 6 (2) (2011), pp.426–437.