Distributed Denial of Service Attacks and Its Counter Measures

Mohammad Jabed Morshed Chowdhury

Among the many security threats in the current Internet, Distributed Denial of Service (DDoS) attacks are considered to be one of the most serious. Denials of Service (DoS) attacks aim to make the resources of the computer system of the victim unavailable or unreliable in providing their intended services. In the context of this work, DoS attacks try to consume and exhaust the victim's bandwidth or the server capacity. In DDoS attacks, the attacker compromises a large number of hosts in Internet and instructs them to conduct a coordinated attack. The network of the compromised hosts is called a botnet. In recent years, a sharp increase in large DDoS attacks has been reported.

While progress has been made in preventing or at least significantly lessening the impact of various security vulnerabilities, real progress in fighting DDoS is still missing. While automated software updates and antivirus programs can limit the number of compromised computers, there are still botnets comprising of millions of nodes. Another potential defence is to filter the packets sent by the DDoS attacker at a firewall after detecting the attack with and intrusion detection system (IDS). These rule-based detection and filtering techniques have not been successful in filtering DDoS attack because the DDoS attacker can send seemingly legitimate traffic. In the case of open services, such as web servers, the DDoS attacker only needs to send large quantities of useless service requests. Thus, there might be no specific features of DDoS attack traffic that the rule-based filters can be instructed to filter. With such malicious but legitimate traffic, DDoS attackers are able to relatively easily bypass most means of DDoS defence.

Different types of DDoS Attack

DDoS attack can be dived into 2 types. One is bandwidth depletion. This method is to congest the network, massive use of the bandwidth then lead the network breakdown. The other type is resource depletion. Attacker depletes the key resources such as CPU, memory and so on and then breaks the serverd. The attack usually starts from numerous sources to aim at a single target. Multiple target attacks are less common. A compilation of different types of DDoS attacks are presented as follows:

SYN Flood Attack

Any system providing TCP-based network services is potentially subject to this attack. The attackers use half-open connections to cause the server exhaust its resource to keep the information describing all pending connections. The result would be system crash or system inoperative.

TCP Reset Attack

TCP reset also utilize the characteristics of TCP protocol. By listening the TCP connections to the victim, the attacker sends a fake TCP RESET packet to the victim. Then it causes the victim to inadvertently terminate its TCP connection.

ICMP Attack

Smurf attack sends forged ICMP echo request packets to IP broadcast addresses. These attacks lead large amounts of ICMP echo reply packets being sent from an intermediary site to a victim, accordingly cause network congestion or outages. ICMP datagram can also be used to start an attack via ping. Attackers use the ping Command to construct oversized ICMP datagram to launch the attack.

UDP Storm Attack

This kind of attack can not only impair the hosts. Services, but also congest or slow down the prevailing network. When a connection is established between two UDP services, each of which produces a very huge number of packets, thus cause an attack.

DNS Request Attack

In this attack scenario, the attack sends a large number of UDP-based DNS requests to a name server using a spoofed source IP address. Then the name server, acting as an intermediate party in the attack, responds by sending back to the spoofed IP address as the victim destination. Because of the amplification effect of DNS response, it can cause serious bandwidth attack.

ARP Storm Attack

During a DDoS attack, the ARP request volume can become very massive, and then the victim system can be negatively affected

Algorithmic Complexity Attack

It's a class of low-bandwidth DDoS attacks that exploit algorithmic deficiencies in the worst case performance of algorithms used in many mainstream applications. For example, both binary trees and hash tables with carefully chosen input can be the attack targets to consume system resources greatly.

Mitigation for DDoS Attack

DDoS countermeasures can be classified as separate techniques for server, network or client based mitigation. In network-based mitigation techniques involves the intermediate network as well as some mitigation methods assisted by client or server subnets.

Congestion Control

Mitigating the effects of a DDoS attack does not necessarily require detection of the attack. A defense mechanism can be effective without knowing whether there is an ongoing attack or not. Applying policies that isolate certain portions of traffic from others can limit the impact of malicious behavior without the need for an attack detection mechanism.

Network Configuration

Several schemes provide protection from DDoS attacks by modifying the physical or logical configuration of a network and its servers. In (Keromytis, 2002), a Secure Overlay Service (SOS) is provided by an overlay network of routers which use a hash-based algorithm to route packets to a server. An outside host wishing to communicate with that server must first contact a Secure Overlay Access Point (SOAP), a designated router that lets a packet enter the overlay only after authenticating its source.

Signature Filters

Signature-based strategies maintain the traditional best-effort routing model of the Internet in normal conditions. The defense system reacts only when an attack detection mechanism flags certain packets as malicious. Based on their reactive actions, signature-based mechanisms fall into two categories: local filtering and traceback mechanisms.

DDoS-Aware Algorithms

There exist simple ways for an operating system to mitigate the effects of a DDoS attack. For example, an OS can periodically scan the TCP connection queue and drop half-open connections. By doing so, the OS prevents a TCP SYN attack from hogging memory resources.

Resource Accounting

Some OS-level resource accounting schemes like Escort (Spatscheck, 1999) are more elaborate than simple DDoS-aware algorithms. They enforce policies which control allocation of time multiplexed resources such as CPU time or network bandwidth ▪