3F-6

Moving Firewall: An Active Networks Application For Defending Against DDoS Attacks

Eric Y. Chen Hitoshi Fuji
NTT Information Sharing Platform Laboratories

Introduction

A denial-of-service (DoS) attack is characterized by the deliberate act of sending a flood of communication to a server in order to block its legitimate visitors by exhausting its bandwidth or resources. A DDoS attack is simply an extension of a DoS attack, in which the flood of communication is launched from multiple hosts toward a server in order to mount a more powerful, coordinated attack. Although we have known of this type of attack for some time, defending against it has been an ongoing concern. This paper presents an effective countermeasure to DDoS attacks.

Current Countermeasures and Issues

Currently, two major technologies have been proposed as countermeasures to DDoS attacks:

1) Cisco's Ingress Filter [1], which is to be installed in every edge router to verify the legitimacy of each outgoing packet's source address. Packets with addresses not matching the edge router's network will not be allowed to go out. This technology prevents DDoS attackers from using forged source addresses.

2) CenterTrack [2], which proposes to install diagnostic routers on the Internet and allow rapid tracking of DDoS floods to their sources, whether their addresses are legitimate or forged. This technology will help victims track down their attackers to their source.

The Ingress Filter has two weaknesses: i) it does absolutely nothing to protect against flooding attacks that originate from valid IP addresses; ii) if the attacker's edge router does not have the Ingress Filter implemented, once packets with forged source addresses pass the edge router successfully, catching them is nearly impossible.

CenterTrack also has a problem within its notification method. Because it knows only the addresses of machines used illegally by DDoS attackers, it can take days to find and speak to all administrators responsible for these machines.

Exploiting Active Networks

The issues mentioned above can be addressed, however, by exploiting a promising technology called Active Networks. Active Networks aims to facilitate the provision of value-added services and to accelerate network infrastructure innovation. It incorporates programmability into intermediate network nodes (routers or switches) and allows end users to customize the way network nodes handle data traffic. Psounis [3] provides an excellent overview on this topic.

Using Active Networks technology, we propose an effective DDoS countermeasure called Moving Firewall. In order to deploy a Moving Firewall, the underlying routers are required to have the following Active Networks capabilities:

1. New functions implemented in standardized modular forms can be injected and executed at runtime;
2. These modules can move among routers as mobile agents do among host machines;
3. A certain amount of bandwidth is set aside from data traffic for module transmission;
4. These modules are authorized to manipulate certain packets, such as those destined to reach the module owner's address.

The Design of the Moving Firewall

Figure 1 illustrates how a conventional stationary firewall fends off a DDoS attack. Assuming that the attackers have been successfully distinguished from the legitimate users, the firewall may effectively free up the server's computing resources by blocking floods from the attackers. However, congestion is likely to occur between routers A and B due to the massive bandwidth consumption. Legitimate visitors will still have trouble accessing the server and, as a result, the attackers will have essentially achieved their goals.

In contrast to conventional stationary firewalls, the Moving Firewall's packet filtering process is not restricted to one location.

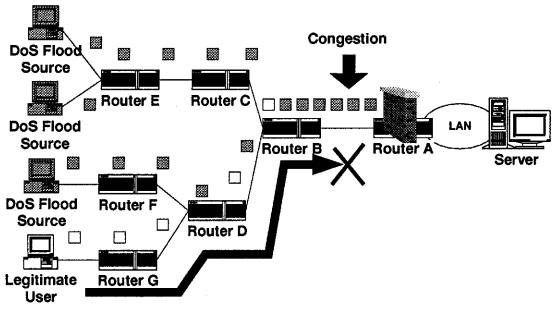

Figure 1: Conventional Stationary Firewall

By exploiting the programmability of Active Networks, the firewall can move to optimal locations to block unwanted packets effectively, while preserving as much bandwidth as possible. Figure 2 illustrates how a Moving Firewall fends off a DDoS attack.

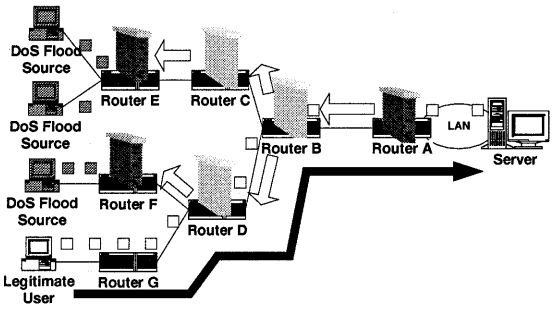

Figure 2: Moving Firewall

Upon detection of the DDoS attack, the parent firewall residing in router A first tries to identify the sources of the floods by using existing technologies such as CenterTrack. [2] It then negotiates with routers (preferably edge routers) near these sources on the paths, makes multiple copies of itself and dispatches these copies (baby firewalls) to target routers E, F and G, which have agreed to host baby firewalls. Figure 3 shows a simplified logic flow of this process. On arriving at these edge routers, the baby firewalls start to block all traffic going from the identified sources to the server. The parent firewall, on the other hand, continues to block residual floods not filtered by baby firewalls. When the DDoS floods terminate, the baby firewalls send log files to the parent firewall and self-destruct. Hence the damage is minimized and legitimate users are allowed to gain access to the server again. In Figure 2, each baby firewall handles 1 to 2 attackers, while in Figure 1 the stationary firewall handles the entire incoming flood by itself. This is an important difference when a typical large-scale DDoS attack occurs, in which thousands of machines are used to coordinate the attack. In principle, the Moving Firewall is a distributed firewall designed to defend against the distributed nature of DDoS attacks.

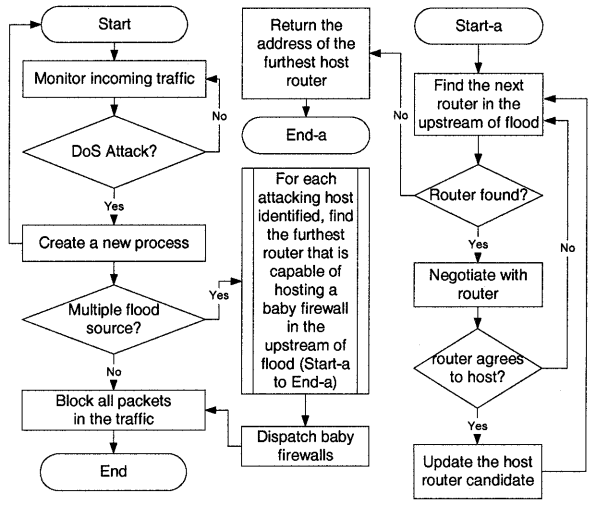

Figure 3: Logic Flow

Conclusions

While existing technologies provide countermeasures against DDoS attacks that use forged source addresses, the Moving Firewall provides an effective defense mechanism against DDoS attacks that use both forged and valid source addresses.

The Moving Firewall does not need to be implemented by the flood sources' edge routers to be effective. By exploiting the programmability of Active Networks, the parent firewall can inject baby firewalls into the flood sources' edge routers at runtime. Alternatively, baby firewalls can also be injected into a transmit router on the path.

Moreover, the Moving Firewall does not require the victim to notify the administrator of the attackers' networks before further action can be taken. The filtering process can be launched automatically at remote locations on behalf of the victim.

References

1. P. Ferguson, D. Senie: "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing" RFC2267, Jan 98.

2. Robert Stone: "CenterTrack: "An IP Overlay Network for Tracking DoS Floods." North American Network Operators Group, Oct. 99.

3. K. Psounis "Active Networks: Applications, Security, Safety, and Architectures", IEEE Comsoc Surveys, 1st Quarter 1999.