Chapter VIII
Distributed Denial of Service
Attacks in Networks

Udaya Kiran Tupakula
Macquarie University, Australia

Vijay Varadharajan
Macquarie University, Australia

ABSTRACT

In this chapter we discuss Distributed Denial of Service (DDoS) attacks in networks such as the Internet, which have become significantly prevalent over the recent years. We explain how DDoS attacks are performed and consider the ideal solution characteristics for defending against the DDoS attacks in the Internet. Then we present different research directions and thoroughly analyse some of the important techniques that have been recently proposed. Our analysis confirms that none of the proposed techniques can efficiently and completely counteract the DDoS attacks. Furthermore, as networks become more complex, they become even more vulnerable to DoS attacks when some of the proposed techniques are deployed in the Internet. The gap between the tools that can generate DDoS attacks and the tools that can detect or prevent DDoS attacks continues to increase. Finally, we briefly outline some best practices that the users are urged to follow to minimise the DoS attacks in the Internet.

INTRODUCTION

Today, enterprises are becoming increasingly dependent on the Internet to perform their business online. Recently there has been rapid migration of several critical applications such as health-care services to the online environment. In addition to the several advantages of the Internet, the stateless nature of the Internet and inherent weakness in the TCP/IP protocol have proven to be very lucrative for several crackers and a great entertainment tool for script kiddies. Since the current Internet architecture is mainly destination oriented, the attacker can easily generate an attack on almost any host/network in the Internet by spoofing the source address.

As organisations and critical applications are becoming increasingly dependent on the Internet to provide their services, even a minor disruption of these services can prove to be enormously expensive and cause severe damage to the organisations. A “denial-of-service” (DoS) [CERT, 2000] is an attempt by attackers to prevent access to resources by legitimate users for which they have authorisation. In the case of Distributed Denial of Service (DDoS) attack, an attacker compromises several hosts on the Internet and then uses these compromised computers to launch coordinated attacks on victim machines. There are no standards to classify DDoS attacks. Mirkovic and Reiher [2004] classified attacks based on the degree of
Distributed Denial of Service Attacks in Networks

automation of the attack tools, exploited vulnerability to deny service, source address validity, attack rate dynamics, possibility of characterisation, persistence of agent set, victim type and impact on the victim.

DDoS attacks are a fundamental challenge faced by the organizations conducting online business today over the Internet. A series of DDoS attacks crippled several major sites like Microsoft, Yahoo, Amazon, FBI in the year 2000. The recent survey by Symantec confirms that 1,000 DoS' attacks of one form or another occur on a daily basis over the Internet. These attacks are ranked among the top 5 security threats for the past consecutive years. Every year, these attacks account to several millions of dollars in lost revenue. Today there is an increased gap between the ease of generation of DoS attacks (with advanced tools) and techniques that are available to counter these attacks.

ATTACK MECHANISM

The DDoS architecture is shown in Figure 1. There can be several handlers in the case of DDoS and each handler is capable of controlling multiple zombies. The attacker does the major part of her/his work in identifying and creating the handlers. The attacker initiates a scan on a number of hosts in the Internet for a known vulnerability. If a vulnerable host is found, the attacker gains root access to the machine by compromising it and install attack tools on the compromised machines. The compromised machines that are controlled by an attacker are called handlers. There can be several handlers in the case of DDoS attacks. The handlers can be randomly located in the Internet and the communication between the attacker and the handlers can be encrypted. There can be several stages in the handler mechanism and the handlers do not directly conduct the attack on the victim machines. As the number of stages within the handler mechanism increases, it becomes more difficult to trace the attacker.

The attacker uses the handlers to further scan and compromise several hundreds of hosts in the Internet. The machines that are compromised and controlled by handlers are called zombies. Each handler is capable of controlling several hundred zombies. The communication between the handlers and the zombies can be encrypted. Zombies are the actual hosts that flood the victim's machine or network with attack traffic. In many cases, the owners of the zombie machines are not aware that their machines are compromised and being used to generate attack traffic on the victim's machines. Since several hundred zombies may be involved in the case of DDoS attack, the victim can experience severe flood of traffic at its end even if each zombie contributes to a small amount of attack traffic. Technologies such as cable modems for home users have further increased the threat of DDoS attacks. This is because with the cable modems the home users are always connected to the Internet and it is easier for an attacker to compromise these systems, which often have weak security. It would be even more difficult to prevent such attacks if the compromised systems attacked with a spoofed source address and constantly changed the attack traffic pattern.

The victim can protect her/his network from the attack traffic at its end by configuring some form of security tools like firewalls or intrusion detection systems. Even if the victim can protect her/his network from the attack traffic, all the victim's network bandwidth is consumed by the attack traffic. So the victim's machines cannot have access to other networks (Internet) and other networks cannot access the victim's network. This will have a considerable impact on the sites conducting online business.

IDEAL SOLUTION CHARACTERISTICS

Before we can consider any solution to thwart DDoS attacks, it is useful to identify and examine the essential characteristics [Tupakula and Varadharajan, 2004] of a robust DDoS solution architecture. Consider Figure 1, where the attacker has already performed a substantial amount of work in creating the zombies. So it is only a matter of few keystrokes for the attacker to launch a severe DDoS attack on the victim's machine/network. An effective approach against these attacks would be to trace the attacker and prevent her/him from commanding the zombies to attack the particular host or network. However, this is not possible with the presently available technology, because often the zombies are controlled by an attack control mechanism or handlers, which is remotely controlled by the attacker. Moreover, the communication between the zombies, handlers and the attacker can be encrypted.

The victim should have a mechanism such as the one shown in Figure 2 to counter the DDoS attacks effectively. In this case, the victim identifies the attack at the point where it occurs but prevents the attack nearest to the attacking source. An ideal solution against distributed denial of service attacks should have the following characteristics:
Related Content

Social Engineering Techniques, Password Selection, and Health Care Legislation: A Health Care Setting
[www.igi-global.com/chapter/social-engineering-techniques-password-selection-and-health-care-legislation/123527?camid=4v1a](www.igi-global.com/chapter/social-engineering-techniques-password-selection-and-health-care-legislation/123527?camid=4v1a)

An Empirical Investigation of an Individual's Perceived Need for Privacy and Security
[www.igi-global.com/article/empirical-investigation-individual-perceived-need/2475?camid=4v1a](www.igi-global.com/article/empirical-investigation-individual-perceived-need/2475?camid=4v1a)

Chinese Wall Security Policy Model: Granular Computing on DAC Model
[www.igi-global.com/chapter/chinese-wall-security-policy-model/23146?camid=4v1a](www.igi-global.com/chapter/chinese-wall-security-policy-model/23146?camid=4v1a)

Modeling Access Control in Healthcare Organizations
[www.igi-global.com/chapter/modeling-access-control-healthcare-organizations/46875?camid=4v1a](www.igi-global.com/chapter/modeling-access-control-healthcare-organizations/46875?camid=4v1a)