Network Intrusion Tracking for DoS Attacks

Mahbubur R. Syed
Minnesota State University, USA

Mohammad M. Nur
Minnesota State University, USA

Robert J. Bignall
Monash University, Australia

INTRODUCTION

In recent years the Internet has become the most popular and useful medium for information interchange due to its wide availability, flexibility, universal standards, and distributed architecture. As an outcome of increased dependency on the Internet and networked systems, intrusions have become a major threat to Internet users. Network intrusions may be categorized into the following major types:

- Stealing valuable and sensitive information
- Destroying or altering information
- Obstructing the availability of information by destroying the service-providing ability of a victim's server

The first two types of intrusions can generally be countered using currently available information- and security-management technologies. However, the third category has a lot more difficult and unsolved issues, and is very hard to prevent. Two very common and well-known attack approaches in this category are the following:

- **Denial-of-Service (DoS) Attacks:** In DoS attacks, legitimate users are deprived of accessing information on the targeted server since its available resources (e.g., memory, processing power) as well as network bandwidth are entirely consumed by a large number of incoming packets from attackers. The attackers can hide their true identity by forging the source IP (Internet protocol) address of the attack packets since they do not need to receive any response back from the victim.
- **Worms:** Worms are self-propagating (do not require user interaction or assistance), malicious codes. They can develop DoS attacks or change sensitive configurations.

Challenges in Network-Intrusion Tracking for DoS Attacks

According to a Computer Security Institute (CSI; 2003) and FBI survey, the total financial loss in the U.S.A. during the first quarter of 2003 due to computer-related crime, which included unauthorized insider access, viruses, insider Net abuse, telecom fraud, DoS attacks, theft of proprietary information, financial fraud, sabotage, system penetration, telecom eavesdropping, and active wiretapping, amounted to $201,797,340. The losses caused by DoS attacks were the highest, amounting to 35% of the total, and were already significantly higher than in previous years. A comparative year-by-year breakdown is shown in Table 1 (Computer Security Institute).

DoS attacks are easy to implement and yet are difficult to prevent and trace. A large amount of money and effort are spent to secure organizations from Internet intrusions.

SOME BASIC FORMS OF DOS ATTACKS

Denial-of-service attacks come in a variety of forms and target a variety of services. Attackers are continuously discovering new forms of attacks using security holes in systems and protocols. Some former

Table 1. CSI/FBI Computer crime and security survey report (in U. S. Dollars)

Year	*2000*	*2001*	*2002*	*2003 (part)*
Total Loss	265,337,990	377,828,700	455,848,000	201,797,340
Loss due to DoS	8,247,500	4,283,600	18,370,500	65,643,300

and very basic forms of DoS attacks, such as the TCP (transmission-control protocol) SYN flood, Smurf attack, and UDP (user datagram packets) flood, are briefly outlined below to clarify the underlying concept.

In TCP SYN flooding, an adversary requests TCP connections by sending TCP SYN (TCP SYNchronization request) packets containing incorrect or nonexistent IP source addresses to the targeted victim. The victim responds with a SYN-ACK (SYNchronization ACKnowledgement) packet to the forged source IP address, but never gets a reply, which leaves the last part of a three-way handshake incomplete. Consequently, half-open connections quickly fill up the connection queue of the targeted server and it becomes unable to provide services to legitimate TCP users.

In a Smurf attack (also known as a Ping attack), the adversary broadcasts ping messages with the targeted victim's source address and multicast destination addresses to various networks. All computers in those networks consequently reply to the source address, flooding the targeted victim with pong messages that it did not request. ICMP (Internet control message protocol) flood attacks use a similar method.

In a UDP-flood attack, a large number of UDP packets are sent to the target, overwhelming available bandwidth and system resources.

Distributed Denial-of-Service Attacks

Distributed DoS (DDoS) attacks are a more powerful and more destructive variation of DoS attacks. In DDoS attacks, a multitude of compromised systems attack a single target simultaneously and hence are more malicious and harder to prevent and trace compared to DoS. The victim of DDoS attacks is not limited to the primary target; in reality all of the systems controlled and used by the intruder are victimized as well.

DEFENDING AGAINST NETWORK INTRUSION

Defense against network intrusion includes three steps: prevention, detection, and attack-source identification.

Intrusion prevention includes the following:

- **Access Control:** Firewalls control access based on the source IP address, destination IP address, protocol type, source port number, and destination port number, or based on the customer need. However, if an attacker attempts to exploit, for example, the WWW (World Wide Web) server using HTTP (hypertext transfer protocol), the firewall cannot prevent it.
- **Preventing Transmission of an Invalid Source IP Address:** Egress filtering of outgoing packets before sending them out to the Internet (i.e., discarding packets with forged IP address on the routers that connect to the Internet) would cease intrusion by outsiders immediately.
- **Increased Fault Tolerance:** Servers or any other possible victims should be well equipped to deal with network intrusions and should work even in the presence of an intrusion or when partially compromised, for example, systems with a larger connection queue to deal with TCP-SYN attacks.

- Intrusion-detection systems (IDSs) continuously monitor incoming traffic for attack signatures (features from previously known attacks). Ingress filtering is performed on the router by the IDS.
- Intrusion tracing identifies the origin of the attack using techniques such as IP traceback.