2.6 Denial of service: amplification attacks

Denial of service: jamming at layer 3

Amplification attack

An **amplification attack** takes place when an attacker is able to use an amplification factor to multiply its power. Amplification attacks are 'asymmetric', meaning that a relatively small number or low level of resources is required by an attacker to cause a significantly greater number or higher level of target resources to malfunction or fail. Examples of amplification attacks include smurf attacks (PING amplification). Amplification attacks are the base for **denial of service** (DoS) attacks.

Smurfing attack

A smurf attack is a **distributed denial-of-service** (DDoS) attack in which large numbers of Internet Control Message Protocol packets (typically used to PING computers within a LAN) with the intended victim's spoofed source IP are broadcast to a computer network using an IP broadcast address. PING is a utility used to test the reachability of a host on a network.

A smurf attack scenario can be broken down as follows:

1. Smurf malware is used to generate a fake PING request containing a spoofed source IP, which is actually the target server address. This will make it look like the source IP address generated the PING requests, even though it did not.
2. The request is sent to an intermediate IP broadcast network.
3. The request is transmitted to all of the network hosts on the network.
4. Each host sends an ICMP (PING) response to the spoofed source address.
5. With enough ICMP (PING) responses forwarded, the target server is brought down.

NTP amplification attack

Another example of an amplification attack is an **NTP amplification** DoS attack. An NTP amplification attack is a DoS attack in which an attacker exploits a Network Time Protocol (NTP) server functionality in order to overwhelm a targeted network or server with an amplified amount of traffic, rendering the target and its surrounding infrastructure inaccessible to regular traffic.

The reference implementation of NTP allows users to request a list of hosts with which the NTP daemon ntpd communicated recently. The list, called 'monlist' has a size limit of 600 entries and contains the IP addresses of the last NTP clients or servers the instance has talked to.

An NTP amplification attack can be broken down as follows.

The attacker uses a botnet to send UDP packets with spoofed IP addresses to an NTP server which has its monlist command enabled. The spoofed IP address on each packet points to the real IP address of the victim.

Each UDP packet makes a request to the NTP server using its monlist command, resulting in a large response.

The server then responds to the spoofed IP address (the victim) with the resulting data (monlist returns max 600 results).

The IP address of the target receives the response and the surrounding network infrastructure becomes overwhelmed with the deluge of traffic, resulting in a denial-of-service (DoS). A response can be up to 206 times larger than the request.