Reflection and Amplification attacks

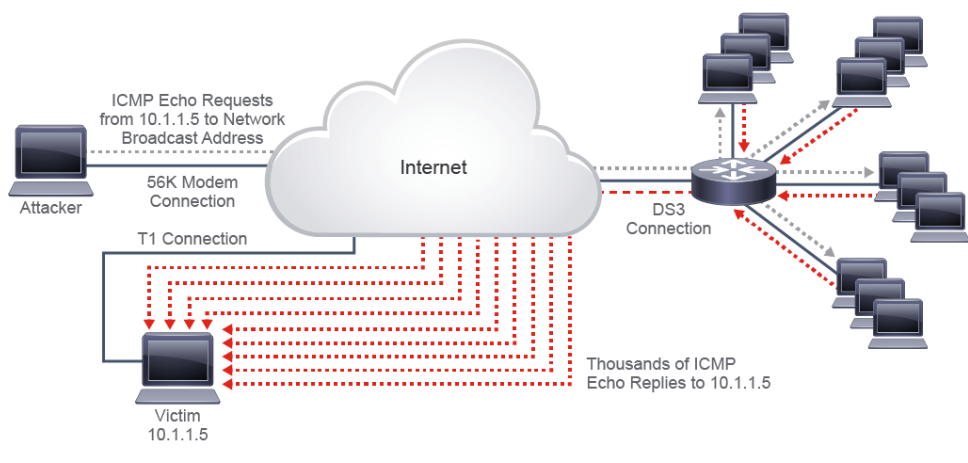
A reflection attack is a type of DoS attack in which the attacker sends a flood of protocol request packets to various IP hosts. The attacker spoofs the source IP address of the packets such that each packet has as its source address the IP address of the intended target rather than the IP address of the attacker. The IP hosts that receive these packets become "reflectors." The reflectors respond by sending response packets to the spoofed address (the target), thus flooding the unsuspecting target.

If the request packets that are sent by the attacker solicit a larger response, the attack is also an amplification attack. In an amplification attack, a small forged packet elicits a large reply from the reflectors. For example, some small DNS queries elicit large replies. Amplification attacks enable an attacker to use a small amount of bandwidth to create a massive attack on a victim by hosts around the Internet.

It is important to note that reflection and amplification are two separate elements of an attack. An attacker can use amplification with a single reflector or multiple reflectors. Reflection and amplification attacks are very hard to trace because the actual source of the attack is hidden.

A classic example of reflection and amplification attacks is the smurf attack, which was common during the late 1990s. Although the smurf attack no longer poses much of a threat (because mitigation techniques became standard practice some time ago), it provides a good example of amplification. In a smurf attack, the attacker sends numerous ICMP echo-request packets to the broadcast address of a large network. These packets contain the victim's address as the source IP address. Every host that belongs to the large network responds by sending ICMP echo-reply packets to the victim. The victim is flooded with unsolicited ICMP echo-reply packets.

The figure below illustrates a smurf attack. Note the differentials in bandwidth of the Internet connections. The attacker has a very small, 56 kbps dial-up connection. The target has a much larger T1 connection (1.544 Mbps). The reflector network has an even larger DS-3 connection (45 Mbps). The small 56K stream of echo requests with the spoofed source address of victim 10.1.1.5 is sent to the broadcast addresses of the large network. As a result, thousands of echo replies are sent to 10.1.1.5 for each spoofed echo, and the target T1 is fully consumed.



Smurf attacks can easily be mitigated on a Cisco IOS device by using the **no ip directed-broadcast** interface configuration command, which has been the default setting in Cisco IOS Software since Release 12.0. With the **no** **ip directed-broadcast** command configured for an interface, broadcasts destined for the subnet to which that interface is attached will be dropped, rather than being broadcast.

Note: An IP-directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet, but which originates from a node that is not itself part of that destination subnet.

While smurf attacks no longer pose the threat they once did, newer reflection and amplification attacks pose a huge threat. For example, in March 2013, DNS amplification was used to cause a DDoS that made it impossible for anyone to access an organization's website. This attack was so massive that it also slowed Internet traffic worldwide. The attackers were able to generate up to 300 Gbps of attack traffic by exploiting DNS open recursive resolvers, which will respond to DNS queries from any host. By sending an open resolver a very small, deliberately formed query with the spoofed source address of a target, an attacker can evoke a significantly larger response to the intended target. Attacks such as this use many compromised source systems and multiple DNS open resolvers, so the effects on the target devices are magnified. The Open Resolver Project cataloged 28 million open recursive DNS resolves on the internet in 2013. DNS operations and DNS-based attacks will be discussed in more details in later sections.

In February 2014, a Network Time Protocol (NTP) amplification attack generated a new record in attack traffic: over 400 Gbps. NTP has some characteristics that make it an attractive attack vector. Like DNS, NTP uses UDP for transport. Like DNS, some NTP requests can result in replies that are much larger than the request. For example, NTP supports a command that is called **monlist**, which can be sent to an NTP server for monitoring purposes. The **monlist** command returns the addresses of up to the last 600 machines with which the NTP server has interacted. If the NTP server is relatively active, this response is much bigger than the request sent, making it ideal for an amplification attack.