A Quick Introduction to Response Rate Limiting

Author: **ISC Support** Reference Number: **AA-01000** Views: **101968** Created: **2013-06-12 18:56**
Last Updated: **2014-04-09 23:44**

0 Rating/ Voters

What is RRL?

RRL, or Response Rate Limiting, is an enhancement to implementations of the DNS protocol that can help mitigate DNS amplification attacks (see KB article AA-00897). In such an attack, the attacker sends high volumes of forged DNS queries to a large number of authoritative DNS servers, using the victim computer's IP address as the source of the request. The victim computer sees huge numbers of replies to questions that it did not ask. The authoritative servers have no way of knowing whether any particular DNS query is real or malicious, but can detect patterns and clusters of queries when they are abused at high volumes. If a goodly number of authoritative servers can all be tricked into sending high-volume replies to the same victim computer, it is quite likely to collapse from overload.

RRL helps mitigate DNS denial-of-service attacks by reducing the rate at which authoritative servers respond to high volumes of malicious queries. The RRL mechanism is part of BIND 9.10, and was available as a software build option in BIND 9.9.4.

The Problem

Any internet protocol based on UDP is suitable for use in a denial-of-service attack, but DNS is especially well suited for such malevolence. There are three reasons:

1. The User Datagram Protocol, or UDP, which is the norm for DNS traffic, was not designed with source validation in mind. DNS server software such as BIND cannot tell by examining a particular packet whether the source address in that packet is real or fraudulent. An attacker can therefore send DNS queries forged to look like they came from the intended victim, causing the DNS server to send the replies to that victim. This is a "reflected attack".
2. Most ISPs do not check for forged source addresses in outbound packets. This allows forged-address reflection attacks to be launched from almost anywhere.
3. Small DNS queries can generate large responses, allowing the attacker to send a lot less traffic than the victim receives, thereby amplifying the attack. For example, an EDNS query for the name `isc.org` of type ANY is 36 bytes long (not counting the wire headers) and triggers a response that is 3,576 bytes long. By using an authoritative DNS server as an unwitting accomplice, an attacker can achieve a nearly 100-fold increase in the amount of traffic that being directed at the victim *and* they can conceal the source of the attack as well.

A Solution

If one packet with a forged source address arrives at a DNS server, there is no way for the server to tell it is forged. If hundreds of packets per second arrive with very similar source addresses asking for similar or identical information, there is a very high probability of those packets, as a group, being part of an attack. The RRL software has two parts. It detects patterns in arriving queries, and when it finds a pattern that suggests abuse, it can reduce the rate at which the replies are sent.

The Results

Operators of large authoritative servers have reported huge reductions in network traffic and server load after enabling RRL. Additionally, these servers are no longer seen as participating in abusive network behavior as fewer illegitimate responses are reaching their intended targets. The impact on legitimate traffic has been minimal.

For more information

KB article AA-00994 outlines how to use the RRL feature in BIND 9.10. As with all BIND features, the complete documentation is in the BIND Administrators' Reference Manual, the ARM. PDF and HTML versions of that manual are part of every release of BIND.