Arming the Defenseless:
An Incentive-based Approach to DNS Reflection Prevention

Casey Deccio
Brigham Young University

The Internet Protocol (IP) has been foundational for the Internet, making inter-network routing of datagrams possible. Yet the fact that IP routing is source agnostic has enabled abuse of the protocol. By spoofing source addresses an attacker can reflect—and amplify—traffic off of public services to unsuspecting victims and effectively overwhelm them, in a class of distributed denial of service attack (DDoS). Spoofing prevention mechanisms have been largely unsuccessful because of the lack of incentive on the part of those required to deploy. We propose a mechanism wherein the parties required to act have incentive to do so.

DNS amplification attacks are a type of reflection-based DDoS attack in which the attackers leverage DNS recursive or authoritative servers to send large amounts of reflected and amplified traffic to their victims. This is done by sending a large stream of DNS queries to these servers, forging the source address of their victims, so the responses are sent to the victims, but with much larger payloads than those of the requests—with the aim of filling the bandwidth of their networks, or otherwise exhausting their resources.

BCP38[1] describes a mechanism wherein Internet Service Providers (ISPs) block outgoing IP packets whose source addresses do not originate within the ISP. As simple as the concept appears, the cost outweighs the benefit for many ISPs. This is particularly true because the ISPs themselves do not directly benefit from this filtering. There is thus no incentive for deployment of BCP38; the only real motivation is community goodwill.

The victim and the reflector have greater incentive to deploy a solution. The victim arguably has the greatest incentive because it is the target. The reflector also suffers unnecessary resource consumption in reflecting the requests, thus becoming a victim of collateral damage incidental to the attack. Additionally, the reflector might have concern about its own reputation, with the reflected responses having the appearance to the victim that the reflector itself is a malicious actor.

Among the solutions proposed to DDoS by DNS reflection are DNS cookies [2], in which the server sends a challenge to the client, which the client must return to the server in its queries. This allows the server to determine whether or not the client is legitimate—and not spoofed. Backwards compatibility remains the challenge—DNS cookies can be deployed on servers, but cannot enforce the use of cookies from unknown clients (i.e., from those that haven't already established themselves as having cookie support).

We propose a mechanism whereby owners of network address space can generally assert and signal capabilities to servers that are would-be reflectors. With this model servers check these capabilities before responding to requests from that address space, so they don't inadvertently become reflectors to victims. This is applied to DNS-based DDoS by 1) a network preparing its DNS resolvers with DNS cookie capabilities; 2) the network advertising the fact that the network supports DNS cookies; and 3) the reflector enforcing DNS cookies upon learning that the network supports DNS cookies. Spoofed packets, for which the cookie sent by the server won't be similarly spoof-able, will be silently dropped, per cookie enforcement policy. This effectively dampens the impact of DNS amplification attacks.

The model herein described can be an effective mechanism to limit Internet protocol abuse by preventing DNS-baesd DDoS attacks caused by IP spoofing. While we have described its application for the DNS, it can similarly be applied to other simple, UDP-based query-response protocols, such as NTP and SNMP.

[1] P. Ferguson and D. Senie. "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing". https://tools.ietf.org/html/bcp38
[2] D. Eastlake and M. Andrews. "Domain Name System (DNS) Cookies". https://tools.ietf.org/html/rfc7873