

# Blocking DDoS Attacks with AS-Based Accountability

David A. Maltz      Daniel R. Simon      Sharad Agarwal  
Microsoft Research

Denial of Service attacks for fun and profit against on-line services are a real and ongoing problem. We argue the best basis for a real solution is *accountability*, meaning that a host receiving unwanted traffic from an entity should be able to ask the network itself to prevent that entity from sending it more packets. Implementing accountability has two components: *identification* of the traffic belonging to the entity to be filtered and *defense* of the attackee by the filtering of unwanted traffic.

Our key insight for implementing accountability is to leverage the existing structure in the Internet - the AS routing graph. Each AS can individually take the steps we outline below to become accountable and recognize benefits from reducing DoS traffic between its customers. However, where ever two ASes who are each accountable peer, they can expand the island of accountability so that all traffic between them is also accountable. We argue proceeding on an AS-by-AS basis is a more plausible deployment story than the router-by-router basis proposed by many other approaches to control DoS.

If accountability could be created, numerous benefits would result. First, once a host detected an attacker, it would spend no further resources (CPU or bandwidth) on that attacker. Second, reputation systems will be enabled: entities that many hosts ask to have filtered will be recognized as entities potentially needing further attention. Third, this notion of reputation rapidly extends in practice to curtailing the value of bot-nets — once a botnet is used to attack a few sites, its members lose their value for attacking other sites.

The next sections outline some desirable properties for Internet accountability and sketch a design of an architecture that holds these properties.

## I. DESIRED PROPERTIES

**Persistence:** Both identity and defense should be persistent. When a site asks for traffic from an entity to be filtered, that request should associated with some persistent attribute of the entity so tricks to change IP address (e.g., DHCP, source address spoofing) cannot evade the filtering.

**Prevent abuse:** a host  $A$  can request that packets from host  $B$  no longer reach  $A$ , but  $A$  should not be able to prevent  $B$  from sending packets to any other host.

**Minimize collateral damage:** If a host  $B$  is attacking  $A$ , then traffic from  $B$  should be dropped but traffic from hosts topologically close to  $B$  should be unaffected. At the minimum, hosts close to  $B$  should have recourse to break their fate-sharing with  $B$ .

**Preserve the any-to-any nature of Internet communication:** Avoid classifying hosts as “clients” or “servers” and allowing only client to server communication.

**No requirement for a global PKI:** Assume that trust (and hence cryptographic signing) exists only between entities that already have a contractual business relationship (e.g., customer-provider, eBGP peers).

**No requirement for new functionality on routers:** Depend only on hardware that exists today.

**Incremental deployability:** The system must not require wide-spread adoption before it provides value to its participants.

**Backward compatibility:** Traffic from hosts that do not participate in the accountability system should see performance roughly equivalent to that of today, where legitimate traffic can sometimes be swamped by DoS traffic, but is otherwise unaffected.

## II. DESIGN SKETCH

An AS that wishes to become accountable takes the following three steps:

- 1) Augment its customer-relationship management software so that every legitimate IP address assigned to a customer can be mapped to that customer’s billing information.
- 2) Implement per-customer ingress filtering, so that every time a customer attaches to the network the source address of its packets can be mapped to its billing information.
- 3) Implement a Filter Request Server (FRS) that accepts requests of the form “host  $A$  does not want traffic from  $B$ .” If  $B$  is directly attached to the same AS as the FRS, the FRS installs a packet filter on the routers where  $B$  connects that drop its packets to  $A$ . If  $B$  belongs to a different AS, the FRS forwards the request towards the FRS in the AS that owns the IP address  $B$ .

We enable incremental deployability using the same kernel of an idea described by Crocker [3]. A bit in the header of the packet indicates whether or not the packet originated in an accountable AS.<sup>1</sup> Packets entering an accountable AS from a non-accountable AS have the *accountable* bit cleared to indicate that the source IP address might be spoofed and that the packets might not stop coming in response to a filter request. Packets transiting between two accountable ASes have

<sup>1</sup>We often refer to this bit as the “evil-bit” in deference to Bellare [1].

the *accountable* bit left unmodified. The *accountable* would be implemented by a bit or reserved-value in the DiffServ Code Point [4] already present in the IPv4 and v6 header. Routers would then be configured to preferentially drop packets having an *accountable* bit of 0 during overload conditions, consistent with the DiffServ architecture [2] that is already supported on most routers and in use in many networks.

More details of our design are available in a technical report [5], including potential attacks against the system and a way to detect ASes that promise to be accountable but then fail to do so.

#### REFERENCES

- [1] S. Bellovin. The security flag in the IPv4 header. Internet RFC 3514, 2003.
- [2] S. Blake, D. Black, M. Carlson, E. Davies, and Z. W. W. Weiss. An architecture for differentiated services. Request For Comments 2475, December 1998.
- [3] S. D. Crocker. Protecting the internet from distributed denial-of-service attacks: A proposal. *Proceedings of the IEEE*, 92(9):1375–1381, September 2004.
- [4] K. Nichols, S. Blake, F. Baker, and D. Black. Definition of the differentiated services field (DS field) in the IPv4 and IPv6 headers. Request For Comments 2474, December 1998.
- [5] D. R. Simon, S. Agarwal, and D. A. Maltz. The “evil bit” revisited : Blocking DDoS attacks with AS-based accountability. <http://research.microsoft.com/~dmaltz/papers/accountability2006.pdf>, October 2006.