The problems associated with operating an effective domain blacklisting system in an increasingly hostile environment.

Robert Gallagher
School Of Computing
Dublin City University

December 13, 2003

Abstract

Bulk mailing, commonly referred to as 'Spamming', is a widely acknowledged problem. Anti-spam 'blocklist' sites have attempted to combat the problem of spam by providing email users and ISPs with dynamic lists of domain names known to harbour spammers.

Several proposals have been made which range from placing levies on email in order to undermine the bulk emailing business model to including a new 'spam' field in email message headers. These solutions would be very difficult to implement on top of the current email system, because of its widespread deployment. They also assume cooperation from the bulk emailers.

This practicum will investigate the problems faced by blocklist systems and propose a solution based around a distributed blocklist system.

Goals

- Case studies of current blocklist systems (Spamhaus, SpamCop)
- Alternatives to blocklisting (SpamAssassin, Vipul.s Razor)
- Investigate history of attacks on blocklists.
- Detail the connection between bulk mailers and virus writers.
- Techniques used by spammers.

The New System

- A distributed network of blocklists, first and foremost.
- A trusted set of submitters (moderators), possibly governed by a recognised standards body, similar to how ICANN functions.
- A small, independent core of servers.
- Versioning and rollback. Removal of mistakenly block sites should be a trivial process; this has been a point of serious conflict between network administrators and blocklist maintainers.
- Modelled on tried and trusted systems: DNS or CVS (Concurrent Version System).
- An answer to the spam 'arms race'?.