A Plan for No Spam
ABSTRACT

The problem of unwanted and irrelevant mass mailings, commonly known as spam is starting to seriously degrade the usefulness of email. In this paper we provide a survey of the principal approaches currently being applied to spam control and propose a strategy by which these mechanisms may be combined to provide a comprehensive solution to the spam menace.

DEFINING THE PROBLEM

Unwanted and irrelevant mass mailings, commonly known as spam are becoming a serious nuisance that if left unchecked may soon be regarded as a Denial of Service Attack against the email infrastructure of the Internet itself.

The term spam is derived from a Monty Python sketch set in a cafeteria in which the principal protagonists have difficulty making them heard above a group of Vikings singing, “SPAM” in honor of the meat product manufactured by Hormel [Hormel]. Although there has been a move, due in part to trademark concerns to use terms such as ‘Unsolicited Commercial Email’ we prefer the colloquial term as being both more familiar and more appropriate.

The defining quality of spam is that it is sent indiscriminately in the knowledge that it will be unwanted by the vast majority of recipients. Unsolicited email is frequently desirable, and in fact it is the problem of distinguishing wanted unsolicited messages from unwanted unsolicited messages that makes the problem of mitigating or eliminating spam so hard.

Certain types of commercial email are also desirable, in particular communications regarding invoices and account balances, newsletters and in many cases certain types of advertisements relevant to the recipient. Calls for Papers and Calls for Participation at academic conferences circulated on computer networks for many years without complaint and in most cases still do.

An ideal spam control system would have the following properties:

• Eliminate all unwanted emails
• Eliminate no wanted emails
• Require no user input on the part of either the sender or receiver
• Be compatible with all uses of email
• Be compatible with all email infrastructure configurations
• Be scalable, that is remain effective if 90% of Internet users adopt it
• Resist attempts to evade it.
• Create no new problems

No perfect spam control solution has been found so far. Filtering approaches are compatible with a broad range of email uses and infrastructure but no filter perfectly identifies even a fraction of unwanted emails without eliminating at least some wanted emails. Furthermore the more widely a filter is used the greater the incentive becomes for the spam senders to test against it to ensure that their spam gets through.
Lightweight authentication approaches based on callback loops are similarly compatible with most email infrastructure and require no intervention on the part of the receiver. Unfortunately the intervention required by the sender is significant and would soon become unacceptable were the solution widely adopted.

Strong authentication techniques based on cryptography offer an approach that can ensure that no wanted email that originates from an authenticated source is eliminated but provides no guide otherwise.

In this paper we consider a plan for spam elimination based on multiple controls. We consider spam to be a security problem; in particular it is an access control problem that requires consideration of both authentication and authorization techniques.

**QUANTIFYING THE PROBLEM**

Another objection to the ‘Unsolicited Commercial Email moniker is that in many cases the subject matter of the spam is outright fraudulent and not commercial in the normal sense. This is demonstrated by the results of a short survey of 89 spam messages received by the author over a 60-hour period (Table 1).

<table>
<thead>
<tr>
<th>Proportion</th>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>35%</td>
<td>Foreign</td>
<td>Mostly Korean, Chinese and Japanese</td>
</tr>
<tr>
<td>21%</td>
<td>Advance Fee/Section 419 Fraud</td>
<td>Invitations to assist in the illegal transfer of large sums of money, usually originating from Nigeria</td>
</tr>
<tr>
<td>7%</td>
<td>Pornography</td>
<td>Several of the examples included explicit images of male and female genitalia and actual sex acts</td>
</tr>
<tr>
<td>6%</td>
<td>Multi-Level Marketing</td>
<td>Multi Level Marketing</td>
</tr>
<tr>
<td>6%</td>
<td>Quack Medicines</td>
<td>Herbal Viagra, Breast, Penis Enlargement</td>
</tr>
<tr>
<td>3%</td>
<td>Bounces</td>
<td>Resulting from account hijacking.</td>
</tr>
<tr>
<td>2%</td>
<td>Credit Repair</td>
<td></td>
</tr>
<tr>
<td>1%</td>
<td>Gambling</td>
<td></td>
</tr>
<tr>
<td>1%</td>
<td>Diploma</td>
<td></td>
</tr>
<tr>
<td>18%</td>
<td>Other</td>
<td></td>
</tr>
</tbody>
</table>

Table 1: Classification of spam received by author 19-21 Jan 2002
The largest single category of spam consisted of messages in foreign languages the author is unable to read and thus categorize further. 29% of the messages corresponded to activities that were outright frauds (Section 419 Fraud, Multi-Level Marketing, Credit Repair). A further 7% corresponded to commercial activities that are at best disreputable and in many instances correspond to actual fraud (Quack Medicines, and Diploma Mills). 8% corresponded to businesses which while not illegal are typically prohibited from sending unsolicited solicitations (Pornography, Gambling). 3% of the unwanted messages were ‘bounces’ resulting from a party attempting to send out spam that purported to come from my email address. This tactic is frequently employed as a means to bypass certain filtering techniques.

The remaining category of ‘Other’ consisted in the main of offers to buy an eclectic range of merchandise including anti virus software, ISO 9000 consulting, information on government grants, sales leads, services to send out spam and small manufacturing plants for the production of small nails, mufflers and hemostatic [sic] clamps. This category consisting of less than a fifth of the total (18%) contained the only offers that could correspond to mainstream commercial business offers. It is not possible to know how many of the offers are genuine and which are merely fronts for identity theft and other fraud.

In addition the sample contained 20 messages where a virus infection had been detected. These are excluded from the survey as any meaningful comparison of the volume of viruses and spam would require a much longer study period as virus infection episodes occur intermittently. Furthermore the fact the attempted infections had been detected indicates that the virus notification could also be suppressed.

While an ad-hoc survey of this type cannot be considered definitive the process is nevertheless instructive in suggesting hypotheses, which might be tested in a broader survey covering a larger number of users and a longer time interval. In particular the following observations were made:

90% of the emails did not have a valid sender address. These emails could be excluded if there were some mechanism that allowed validation of sender addresses.

1/3rd of the emails were not correctly addressed to the recipient. These messages could be excluded by simply enforcing the RFC822 message standard that requires every message to have a valid To: CC: or BCC: field identifying the recipient, making adjustment where necessary to account for messages relayed through mailing lists.

1/3rd of the emails were in a foreign language. These messages could be excluded by simply detecting the language or even the character set in which the message was written and excluding messages in languages the recipient could not read.

1/5th of the spam has content that is similar to legitimate content. It will be hard to classify on content alone without content filters that have a great deal of knowledge about the individual recipient.

At least 1/3rd of the spam is being sent by organized crime. However a significant proportion of spam is generated by businesses that at least meet the semblance of respect for the law.

There is a considerable range of expertise demonstrated by the spam senders. In many cases the senders actions defy common sense, what is the point of sending the same person 19 proposals involving 6 different dubious financial schemes in a 60-hour period? Surely even the dimmest mark is going to suspect something.

Forged email address headers are being used to attempt to bypass existing whitelist techniques.
Again further study is necessary before firm conclusions are drawn. It is in any case necessary to treat such survey results with some care however since as the sample itself demonstrates the spam senders are constantly adapting their techniques to blunt the effectiveness of countermeasures.

While 33% of spam messages in the sample do not meet the minimal requirement of a valid recipient address. We cannot infer from this fact alone that blocking all messages of this type would reduce spam volumes would remain effective at blocking 33% of spam since it is not difficult for the spam senders to add them.

We should not conclude that all such mechanisms are intrinsically hopeless however. It is unlikely that Korean spam senders attempting to sell goods to a Korean audience would switch to English in response to widespread deployment of filters to block foreign language spam. The spam senders adopt the tactics they do out of necessity, in many instances to avoid detection. While each anti-spam mechanism on its own may be vulnerable to counter-strategies, evasion becomes increasingly difficult as more anti-spam techniques are employed.

The lack of sophistication demonstrated by many of the spam senders suggests it is likely that even naïve mechanisms such as filtering to eliminate messages that do not meet the requirements of RFC822 would retain a certain degree of effectiveness for a considerable time. In many cases the spam senders use off the shelf packages that send bulk email whose internal workings they do not understand. These so-called 'list-kiddies' will typically buy a CDROM of email addresses through a spam advertisement and send out as many messages as they are able to until their ISP terminates their account.

The degree of linkage between spam and organized crime is debatable. While messages touting section 419 frauds and multi-level marketing schemes are clearly frauds run by organized crime on a significant scale it is impossible to determine from the other messages whether the party sending it is dishonest or merely disreputable. Anecdotal evidence suggests that many offers of goods for sale are fronts for various types of credit card fraud.

A large number of spam messages defy easy explanation. Many messages purport to advertise goods for sale but provide no means of contacting the vendor. A possible explanation for these messages is that they are attempts by providers of spam software and services to demonstrate that ‘spam marketing really works, or why else would they do it’.

Another possible explanation is suggested by the business practices of some of the providers of spam services, accepting payment, often in cash from offshore entities with dubious credentials. This behavior is often associated with front businesses used for money laundering.

**The Scams behind the Spams**

As research by the Federal Trade Commission [FTC1], a large proportion of spam messages sent are connected to some form of fraud. The ‘scams behind the spams’ are varied in nature, from the section 419 advance fee frauds mentioned earlier to pyramid schemes and various forms of consumer fraud. These online frauds are invariably e-commerce variants of existing frauds, the section 419 frauds being a modern version of the ‘Spanish prisoner’ confidence trick that appeared in the 1920s.

Solicitations for goods are frequently fronts for identity theft. Once the user enters their credit card details they will be used to purchase more than the customer intended. Another identity theft technique seen recently is forged emails that purport to come from EBay, requesting that the recipient ‘verify their account status’.
In some cases the spam sender is genuinely offering goods for sale, the goods just happen to be stolen. This is typically the case where offers for ‘anti-virus’ software offered at steep discounts are concerned.

Offers to ‘work from home’ are frequently pitches for pyramid marketing schemes. Chain letters also circulate via spam. This scam has recently mutated into a new form called grid marketing. The customer is offered the chance to buy a $5000 Plasma TV or similar expensive item for a fraction of its true cost by buying a spot on a ‘grid’. When all the spots on the first grid are sold the first person on the grid gets their TV. When all the spots on the second grid are sold the second person on the first grid gets their TV. The catch is that only a small fraction of the customers who hand over their money will ever receive a TV.

SECOND ORDER PROBLEMS

The cost of spam is not limited to the direct costs of delivery and wasted time. In addition the indirect costs of ad-hoc spam ‘solutions must also be considered. These include:

- Lost email.
- Processing of mail bounces.
- Vigilante actions.

Lost Email
The most immediate second order problem due to spam felt by the user is when email is lost either by being overlooked in the sheer influx of spam or by being incorrectly identified as spam by a spam filter. As a result of this type of attrition few enterprises have confidence in email as a transport mechanism for ‘must deliver’ messages such as invoices and accounts.

Mail Bounce Storms
Another serious second order problem is the processing of mail bounce messages that result when a spam sender attempts to send a message to an address that is invalid. It appears that this mechanism has been used in some cases to mount a ‘Denial of Service’ attack against the mail servers of an ISP. The attacker sends a large number of messages with a forged email address to a large ISP with the intention of swamping the mail servers of a smaller ISP.

Mail Bounce Storms
Another serious second order problem is the processing of mail bounce messages that result when a spam sender attempts to send a message to an address that is invalid. It appears that this mechanism has been used in some cases to mount a ‘Denial of Service’ attack against the mail servers of an ISP. The attacker sends a large number of messages with a forged email address to a large ISP with the intention of swamping the mail servers of a smaller ISP.
**Vigilante Actions**

Vigilante actions range from passive mechanisms such as blacklists to direct interventions such as mail bombardments. For the purposes of this article we deem any mechanism that lacks accountability to be a vigilante action.

Vigilante actions dilute the rule of law; the individual is held accountable to the mob with no recourse. They are also ineffective since they frequently miss the intended target. Vigilante action in the form of mail bombardments in response to spam did not result in a reduction in the volume of spam, it merely led to the senders using false addresses so that the mail bombardments would hit someone else.

Another form of vigilante action is the so-called ‘teergrubbing’ attack in which an email server that believes a message being sent is spam will respond by slowing down responses in an attempt to consume the spam sender’s resources. Such techniques are unlikely to be effective since the ability to quickly identify and terminate slow connections is an obvious requirement for any bulk email system.

**Blacklists**

While there is general agreement that active vigilante mechanisms that attempt to attack the user should be generally discouraged no similar consensus has yet emerged concerning ‘blacklists’. These are commonly used by ISPs as a method of controlling the amount of spam received. However this use can lead to a user’s email being silently blocked. An issue that has led to complaints from the ACLU and numerous others [ACLU].

Blacklists emerged as a means of coercing ISPs to terminate accounts of users who were ‘known spammers’. Blacklists of IP addresses of alleged spam senders were circulated and ISPs were encouraged to block email originating from the blacklists. As spam senders were forced to develop new ways to disguise the origin of their posts new blacklists began to appear claiming to list open relays, email servers that will forward messages indiscriminately from any sender.

Proponents of blacklists have argued that the mechanism is consensual since the choice to filter on the basis of the blacklist lies with the ISPs that subscribe to them. While the blacklist maintainers appear to take great care to avoid criticism by referring to coercive techniques through code words such as ‘education’, it is instructive to examine the language used by maintainers of blacklists to describe each other; here the code words are dropped. SPEWS describes MAPS as “Great for putting pressure on an ISP.”

Blacklists can only work as long as the Internet community generally can have confidence in the way they are run. Unfortunately the majority of blacklist operators appear to consider themselves beyond accountability. None of the blacklist maintainers describe a dispute resolution procedure; most do not even provide a contact address. In at least one case a blacklist demands a deposit of $1,000 before investigating any compliant about a blacklisting, the decision as to whether the blacklisting was unfair and the deposit returned resting with the recipient alone. Such practices border on extortion.

In many cases the blacklists describe themselves as being ‘high collateral damage’. This is where the most clear-cut cases of abuse by blacklist operators tend to occur. In one recent incident one of the blacklists listed the entire nation of China. Another blacklist listed UUNET, one of the largest ISPs in the US including all its customers in an attempt to force UUNET to shut down a Website run by a UUNET customer. These are the actions of self-appointed censors, not guardians of the public interest.
Email Address Harvesting Attacks

Spam senders use a variety of techniques to obtain email addresses. In a dictionary attack the spam sender simply selects a mail server and tries a list of common account names such as ‘alice’, ‘bob’, etc. in turn, and records which account names are accepted and which are rejected.

Another common tactic is to use robots to search the Web for email addresses. Research by the FTC [FTC3] has shown that any email address that appears on a Web page is likely to be abused by a spam sender. The spam senders do not appear to take any notice of the context in which the names appear. An email address appearing on a Web site aimed at children is as likely to be bombarded with hardcore pornographic images as any other. Chat rooms are particular targets of harvesting attacks; the FTC researchers received a spam message to an email address within seven minutes of it being used in a chat room.

Once harvested there is no limit on the length of time an address is used. In a recent test a number DNS domains that had been out of use for many years were brought online again and started receiving large volumes of spam almost immediately. Harvested addresses are often sold on CDROM, a typical price being $20 for a CDROM with 10 million addresses. Once an address is listed on a CDROM it is likely to receive large volumes of spam until a solution to the spam crisis is found.

An email harvesting technique that is being used increasingly attacks archives of mailing lists on the web. The harvester records the addresses of each poster and uses them to provide both sender and recipient addresses. This attack results in the spam recipients receiving email that appears to come from people they know, bypassing many types of filters and increasing the chance that the message is read. Unless the spam recipient is aware that email is insecure they are likely to conclude that the spam came from its purported sender, resulting in misplaced disgust, anger and in some cases threats of lawsuits.

Email address harvesting has had a significant impact on the use of the net. Ten years ago users were encouraged to publish their email contact information in forums such as Usenet. Today users are being warned to keep their email contact details private in case they are hijacked by a spam sender [FTC1]. The result has been a chilling effect on online discourse. What were once public meeting places that led to private conversations are now forums for exclusively public discussion with no opportunity for private conversation.

LOST OPPORTUNITIES

The cost of spam is not limited to its direct impact and the cost of the mitigation strategies employed. The greatest cost of spam may well be the immeasurable cost of lost opportunities. If no way is found to reduce the level of spam to acceptable levels ordinary users will start to stop using the Internet.

Despite the breathless journalistic prose describing the concept of ‘internet time’ popular in the late 1990s, Internet technology like any other takes time to move from theory to being ubiquitous. Much of the potential of the Internet is so profound that it is inconceivable that the social and business changes required could take place in a few months or even years. Change on this scale takes decades or even generations.
A quarter of a century after the arrival of the low cost Personal Computer and a decade after the arrival of the World Wide Web, many clerical workers spend their entire working life doing nothing but take information generated by one computer system and manually enter it into another. Each day tens of millions of utility bills are sent to consumers, who must manually sort them out of their postal junk mail, open them and pay them. The movement of this type of data to the Internet is long overdue; the infrastructure to communicate that information securely is now in place. But that transition cannot take place if consumers are now afraid to open their email inbox for fear of what might lurk inside.

**EMAIL INFRASTRUCTURE**

The email infrastructure in use today has evolved over a thirty-year period. Although the vast majority of mail is now sent using the SMTP protocol (more than 99%) legacy systems such as X.400 and UUCP still exist. Evidence that these systems are still in use is provided by the fact that attempts to remove support for these systems results in strident complaints from individuals claiming that they are still necessary serve a significant constituency that is apparently technically sophisticated enough to use email but not sophisticated enough to use 1980s technology.

SMTP is one of the oldest and most widely used Internet protocols. Consequently SMTP deployments vary considerably according to the precise vintage of the protocol implemented. For example the originating machine may send a machine in (at least) the following ways:

- The originating machine sends the email directly to an email server at DNS address example.com.
- The originating machine sends the email to an email server identified in an mx record in the DNS domain example.com.
- The originating machine forwards all messages to an email server with a DNS address corresponding to the sender's email address, which forwards the message to the specified destination.
- The originating machine forwards all messages to an email server with a DNS address that does not correspond to the sender's email address, which forwards the message to the specified destination.

This variation results in frequent objections being made to spam control schemes that assume that a particular SMTP deployment is adopted. Such objections clearly have weight in cases where the spam control scheme assumes that all users have adopted a particular scheme but have less weight when it is asserted that a scheme should be rejected since a user with an obscure email configuration could not use it.

**Mailing Lists**

A mailing list receives a message from one recipient and forwards it to a list of recipients. Mailing lists thus serve as amplifiers for email messages. A spam sender can send a single message to a mailing list and reach an audience of hundreds or thousands.

Despite the widespread use of mailing lists the SMTP protocol does not provide an explicit architecture for their use. As a direct result (in my personal opinion), the issues raised by interactions between mailing lists and the SMTP protocol are so numerous that a comprehensive treatment would require a book length treatment at the very least. Some assert that the SMTP protocol is designed to interact with mailing lists and that these problems are the sole fault of implementations. There must however come a point where such faults are considered the responsibility of the specification authors.
Unwanted mailing list subscriptions can in themselves be a form of spam. One of the earliest problems that arose from the use of mailing lists was the 'mail bombing' attack where an attacker would mount a denial of service attack by subscribing the victim to a large number of mailing lists. The mailing lists could also be subscribed to each other so that a single post sent to one mailing list would result in tens of thousands of messages being sent to the victim.

As a result of this and similar attacks mechanisms were developed that performed authentication of the subscriber in subscription requests and restricted mailing privileges to mailing list subscribers.

Mailing lists are also used as spam relays. One of the principal problems with mailing lists with respect to spam is that an email from a mailing list comes from a source that the subscriber has chosen to receive email from. As a result such messages are more likely to be read than messages from anonymous sources.

In response to rising levels of abuse, many mailing lists are now moderated purely for the purpose of preventing spam abuse. This is generally considered undesirable as it creates a time consuming task for the moderator and introduces a delay in posting to the list. It no longer suffices for posting privileges to be restricted to mailing list subscribers since spam senders will frequently subscribe to the list to gain posting privileges. Alternatively the spam senders sometimes forge email headers so that a message appears to come from an authorized poster.

**Gateways**

Another class of email infrastructure that must be considered is email gateways that provide an email interface to other protocols such as the Usenet NNTP protocol and legacy email protocols such as X.400.

**Infrastructure Changes**

Many spam control proposals start from the proposition that the email infrastructure is fixed and unchangeable. A brief survey of the numerous changes in the email infrastructure over the last ten and the last twenty years shows that on the contrary such changes are constantly taking place.

Certain types of change are easier to establish than others, however. In particular infrastructure changes that require widespread adoption by clients before they can be deployed at servers are particularly hard to achieve. Infrastructure changes that can be unilaterally deployed by either servers or clients and provide an immediate value to the party deploying them are achieved considerably faster.

**Towards Solutions**

As we have shown in the previous section, there are many types of spam and it is likely therefore that any realistic program to eliminate spam will have to address the problem in multiple ways. In particular we should not reject a mechanism out of hand simply because it fails to deal with a particular type of spam sender. For example it is highly unlikely that spam senders engaged in organized crime will respect opt-out lists or legislative approaches. We should not however, conclude from the fact that a mechanism fails in certain circumstances that it fails completely in all circumstances.

The only mechanisms that we rule out of hand are those based on vigilante actions that attempt to gain compliance by coercion.
BEST PRACTICES

The traditional response of the Internet to problems caused by problem users and administrators of deployed protocols is to specify some form of 'Best Practices'. Spam is an attack on the Internet community. The short survey and prosecutions by the FTC and others show that the spam senders are in many cases outright criminals, how then can best practices help?

One area in which best practices can provide concrete benefit is in ensuring that the vast majority of Internet users who are acting in good faith do not inadvertently make the problem worse by poorly chosen or poorly coordinated mitigation strategies. Many of the problems being caused by irresponsible blacklists could be addressed through common agreement on best practices for blacklists setting out criteria for issues such as notice to the listed parties, appeals processes and the acceptability of ‘collateral damage’. While such a statement could not by itself compel responsible action by the blacklist maintainers it is likely that network administrators would quickly stop subscribing to blacklists that did cross whatever line was drawn.

Best practices can also provide backing for legislative approaches. An appropriate statement by an authoritative body can help a court to decide that a particular form of behavior is unacceptable. Even if such statements do not have the endorsement of a legislative body they can quickly acquire the force of law when the worst malefactors are being dealt with.

Acceptable Use Policies

Perhaps the most important anti-spam measure to date has been the adoption of acceptable use policies that prohibit sending of spam by Internet service providers of all types.

Such use policies do not just protect the other users of the Internet; they protect the Internet service provider against abuse by their own users. In a recent case a university discovered that some of its students had been renting out the use of their machines to spam senders, seriously degrading the network service for all the users.

Pull Vs Push

As previously mentioned, one of the major problems caused by spam is false positive identification as spam of legitimate emails. This is a particular problem with commercial mailing lists and newsletter messages requested by the recipient which frequently carry advertising and make use of content that is likely to be flagged by content inspection filters as spam. While some have argued that the commercial nature of these emails means that this type of false positive is unimportant it seems odd to consider the loss of messages specifically requested by the user to be less important than the loss of unsolicited personal emails.

The core problem with these messages is that although the sender and recipient know that the user has consented to receive the messages, there is no way for that consent to be communicated to the mail infrastructure that transports the message.

One possible solution to this problem would be to add some form of authentication mechanism that communicated the recipient’s consent to the mail infrastructure. This is unlikely to prove practical in deployment however since any benefit would require changes to all parts of the email infrastructure – clients, originating servers and receiving servers.

Another option would be to distribute this form of content using the pull model of the Web [HTTP] and NNTP [NNTP] rather than the push model of email. In the pull model no content is sent until the client specifically requests it. Consent is thus implicit in the pull request since the client will not request content unless directed by the user.
For the pull model to become practical a number of difficulties must be overcome. The most important of these being obtaining a commitment from the major software client to supporting the protocol in the commonly used email clients. A mechanism is also required that tells the client where the updates will be available from, the expected frequency of those updates, the format etc. The Really Simple Syndication (RSS) Protocol [RSS] appears to have these properties, although it is currently being applied in a different domain.

**Opt-out and Do-not-spam lists**

Many spam messages carry a 'click here to opt-out' option. Research by the FTC has demonstrated that a large proportion of these opt-out options are bogus [FTC3] and it is not possible for the user to connect to the opt-out site. Opt-out schemes of this type are unacceptable however, even if spam senders observe them since the spam victim is required to opt-out with each spam sender individually. This is an impossibility if the victim's email address has been listed on a CDROM that has been sold to several thousand spam senders. For opt-out to be practical it must function in the same way that state do-not-call telephone lists do, the address owner opts out once and it is the responsibility of the spam senders to ensure that their lists are clean.

Opt-out lists have proven to be of value in controlling the volume of unsolicited mail and unsolicited telephone calls from legitimate businesses. We note that a significant proportion of spam is sent on behalf of legitimate businesses that may be considered likely to respect such matters. Certainly a mechanism of this type widely deployed would deprive spam senders of the claim that they respect opt-out requests.

A more powerful argument against opt-out lists is that it is likely that spam senders would routinely abuse lists of opted-out email addresses as a source of email addresses. This objection may be addressed by appropriate use of cryptography in which the entries in the list are obscured using a one-way message digest function such as SHA-1. The opt-out list consists of a sequence of message digests of the opted-out email addresses sorted by the message digest value to permit rapid lookup by binary search or similar means. A spam sender may use the list to determine whether an address has been opted-out but cannot use the opt-out list as a source of target email addresses.

One objection made to the scheme above is that spam senders might use the list to validate email addresses to determine whether they are valid or not. This objection does not take account of the fact that the costs of using invalid addresses are not borne by the spam sender alone and result in the 'bounce storm' problems mentioned earlier. A high proportion of delivery failure events does not appear to deter spam senders. One way to eliminate this objection would be to seed the list with a large number of false addresses that spam senders are attempting to send spam to.

**Accountability**

One of the major difficulties faced with distinguishing legitimate bulk senders from illegitimate ones is the difficulty of determining whether the claims made that the bulk sender observes a particular set of best practices is true or not.

This problem also faces the bulk senders themselves. At present there is no way that a outsourced provider of bulk mail services can tell if the email addresses on a list a customer wants used for a mailing have in fact opted-in as is claimed.

Technical mechanisms are required that enable this form of accountability to be achieved.
CONTENT INSPECTION

Aspirin will not cure a cold but it will relieve the symptoms and make the cold more tolerable. Content inspection has a similar effect on spam. The symptoms of spam are relieved to a considerable degree, but the patient is still under attack from the infection.

Content inspection is a form of spam filtering that uses the content of the messages as the basis for the decision to filter. One of the principal difficulties with content inspection mechanisms is the ease of evasion by spam senders. If the spam sender knows the criteria applied by the content inspection technique she can construct her messages so that they are not caught.

There are many forms of content inspection, each of which has advantages and disadvantages:

Naïve Keyword Inspection
Messages are scanned for the presence of words or phrases that occur frequently in spam messages such as penis, HGH or multi-level marketing. This type of filtering is implemented in many common email clients such as Outlook [MSFT]. Keyword inspection alone is simple to implement but tends to have very high rates of false positives. A recent attempt to deploy a keyword inspection based mechanism at the UK House of Commons resulted in many emails concerning the Sexual Offenses Bill to be rejected as obscene [BBC].

Naïve Language Inspection
The Internet is an international medium and spam is sent in many languages. As a result a large number of spam messages are completely incomprehensible to the reader. While fully understanding the meaning of a mail message is a complex problem that is AI complete, that is it requires a solution of the artificial intelligence problem, detecting the language that the email is written in is considerably easier. In many cases the character set in which the email is sent may be used as a proxy for language, although this technique can result in false positives as a Japanese user may send all their messages in a Japanese character set, using the ASCII subset for messages in English. Another problem with language inspection is that large software vendors would face a considerable from foreign users of their product if they introduced language sensitive filters in their products.

Keyword Inspection with Statistical Techniques
The effectiveness of keyword inspection can be substantially improved if combined with statistical techniques that assess the probability of a message being spam based on the presence of multiple keywords. Various techniques may be used for this including Bayesian inference and least squares approaches. While such schemes can show impressive results in tests the practical effectiveness of these techniques in widespread tends to be much more limited due to countermeasures employed by the spam senders.

Keyword Inspection with User Feedback
There has been considerable recent interest in content inspection mechanisms that employ user feedback, in most cases in combination with some form of Bayesian inference [PG1][PG2]. This approach provides some resistance to spam sender counter measures since the individual users maintain separate databases of desirable and undesirable messages. The drawback to this approach is that it requires user intervention on a per message basis which experience demonstrates limits the effectiveness of the scheme severely.
**Keyword Inspection with Dynamic Update**

Another approach to improving the effectiveness of keyword inspection is the combination of statistical techniques with an online source that provides regular updates. This approach is frequently combined with the template approach described below.

**Dynamic Template Response / Fuzzy Matching / Checksums**

Dynamic template response (also known as fuzzy matching) uses templates or ‘fingerprints’ of known spam messages to identify spam messages [DCC]. The templates are constructed using spam messages sent to ‘honey-pot’ email addresses, either by hand or using some form of automated tool. While this technique can be very effective it is also costly to maintain, particularly since the spam sender may employ countermeasures that cause each spam message to be slightly varied.

Content inspection techniques that are successful on a small scale frequently fail when applied on a large scale due to the countermeasures taken by the spam senders. Microsoft Outlook provides a simple content inspection mechanism based on keyword identification. For a content inspection technique to be effective on a large scale it must adapt to the evasion strategies of the spam senders. Instead of providing an aspirin, effective content inspection techniques tend to provide the equivalent of long term palliative care, the symptoms are eased but only with continuous effort and the underlying disease is never cured.

**AUTHENTICATION AND AUTHORIZATION**

Practically all spam messages sent today attempt to evade anti-spam measures by use of false header information. None of the spam messages that were examined in the writing of this paper carried a genuine sender address. Most of the messages contained from addresses that were obviously fake. In some cases the addresses were not even valid. Some contained no sender address at all. This suggests that a robust method of detecting false sender addresses would provide an effective means of eliminating spam.

Detecting false sender addresses would be a simple task but for the fact that the SMTP protocol allows a sender to forge a message that purports to come from any sender. The security risks of this failing were demonstrated in 1993 when Adelyn Lee, an executive assistant at Oracle filled a sexual harassment lawsuit against Larry Ellison alleging that Ellison had threatened to fire her if she did not have sex with him [Oracle]. Ms Lee initially won an out of court settlement of $100,000 after producing an incriminating email that purported to come from Ellison. A few months later however evidence was discovered that proved that the Ellison letter was a forgery. Ms Lee was convicted of perjury, falsifying evidence and breaking into a computer system and sentenced to a year in jail.

The use of forged email addresses is currently rare but becoming more common. A particularly insidious spam sender trick borrowed from the Klez computer virus is to harvest email addresses from mailing lists archived on the Web and send large numbers of emails purporting to come from one member of the list to the other members of the list.

The use of forged email addresses is likely to become very common if the use of anti-spam filters that detect missing or obviously false from addresses becomes common. To address this problem, some form of authentication scheme is required that provide an unequivocal proof that the sender address is valid.
A spam sender might attempt to circumvent an authentication scheme by sending messages with a legitimate, authenticated sender address. We find this objection to be a weak one since it is clear that spam senders have a considerable motivation to conceal their identity. If every email carried an authenticated sender address spam senders would be forced to obtain new DNS addresses frequently to conceal their identity, increasing costs significantly.

**Authentication**

Authentication techniques are broadly divided into two types, network based and cryptographically based.

**Network Level – IP based**

If a mail server knows the set of all possible IP addresses from which an email with a particular sender address is known the IP address may be used to provide a lightweight means of authenticating the email sender. This mechanism is not completely reliable since an IP address can be spoofed albeit with somewhat more difficulty than spoofing a sender address.

The principal difficulty with using IP based authentication is discovering whether an IP address is a valid source for a particular sender address. Some mail servers use the reverse DNS, which maps IP addresses to domain names for this purpose. This approach only works if the email is sent via a mail relay that is configured with reverse DNS entries for the domain of the sender address.

**SMTP Routing information:**

An SMTP message carries information that describes the path it has taken from one mail server to another. This routing information may in some circumstances be used to determine whether the message did come from the purported source.

**Message Identifier Matching:**

A mail service may use the In-Reply-To and References headers to identify messages that are replies to messages that originated at that service. Construction of the original message identifiers using a secret key and Message Authentication Code allows this to be achieved without the need to maintain a list of all message identifiers issued by the service.

**Callback loop, Challenge/Response:**

When an email is received a message requesting confirmation is sent to the purported sender address. If the confirmation message is received the sender address is considered to be authentic. The callback loop mechanism is unusual in that it is an active authentication mechanism that is applied at the request of the receiver rather than being applied passively to every message by the sender.

**Cryptographic – SSL**

An extension to the SMTP protocol allows the use of the Secure Socket Layer (SSL) via the STARTTLS operation [StartTLS]. SSL allows authentication of both the sending and receiving email servers using X.509 digital certificates. Although SSL allows the email relay to use any IP address without the need for configuration of a reverse DNS address the sender must send their outgoing mail via a relay.

**Cryptographic – S/MIME**

S/MIME provides end-to-end authentication of the sender address and message body [SMIME]. The sender need not send their message through any specific email relay.
Trusted Hardware – Velocity Indicator
Widespread availability of trusted hardware platforms such as TCPA and Microsoft’s Palladium will make a new form of cryptographic authentication possible, a velocity indicator which informs the recipient of an email message that the message was authenticated by a trusted platform and the rate at which the trusted platform was performing authentication operations. A message bearing a velocity indicator that shows a very low rate of authentication operations is unlikely to be spam [PHB].

Authentication Policy
For a passive authentication mechanism to be useful as a means of detecting forged sender addresses it is necessary to know whether a purported sender has a policy of using authentication. Otherwise the recipient is unable to distinguish a message from a user who does not use the authentication mechanism from a forged message purporting to come from a user who always uses an authentication mechanism.

The Internet architecture does not include a mechanism designed for the purpose of communicating security policies. Fortunately the DNS architecture provides the necessary functionality and may be readily adapted to the purpose without putting an undue load on the DNS. The Security Policy Advisory Mechanism provides a set of DNS extensions that address this need [PHB2].

The principal disadvantage of using the DNS as a means of communicating security policies is that the DNS itself is insecure. DNS Security [DNSSEC] promises a mechanism that will provide security for the DNS if the working group developing it ever arrives at a deployable version of the protocol. Fortunately the security weaknesses of the DNS do not lend themselves to exploitation on the scale necessary to make exploitation of these weaknesses a viable means of defeating an authentication based anti-spam measure.

Indiscriminate Callback Loop Schemes
Callback loop, also known as challenge/response schemes if widely deployed may rapidly become as great a nuisance as the spam they are meant to control. In effect the user of the callback loop reduces the amount of spam they receive by creating spam for everyone else that attempts to send them a message. If every message resulted in a callback loop, half the email received by every email callback spam.

Most callback loop mechanisms support some form of whitelist that causes messages sent by that person to be accepted without further callback authentication. Unfortunately many users of callback loops appear to consider putting correspondents on such whitelists to be a rare privilege rather than a common courtesy. In many cases the callback loop services do not automatically whitelist replies to messages the users send. So a person may receive a request for help from someone, go to some trouble to give an answer and then find that the answer is rejected unless they also answer a callback loop. This type of discourtesy is completely unnecessary if the message identifier matching authentication technique described above is used.

Another problem with some callback loop schemes is that they are indiscriminate. If a spam sender uses a forged email address as the source of a spam message a callback loop will query the forged address causing the owner of the forged address to be mail bombed.
Yet another problem with these schemes is that their behavior is unpredictable when one user of a callback scheme tries to contact a user of a different callback scheme. In some cases the user’s messages get through, in others each rejects the requests of the other. In quite a few cases the users of the same callback loop scheme are unable to exchange email.

While many consider the indiscriminate use of callback loop schemes to be anti-social, their use as a last resort when a message would otherwise be dropped is generally considered acceptable. The unintended side effects of callback loops may be avoided by means of protocol markings identifying callback requests as such and by resorting to callback loop authentication only when no other means of authentication is available.

**Authorization Mechanisms**

Spam is a resource allocation problem. When email was first invented computer communications were slow and access was limited to a small number of users. The only limit on the number of messages a spam sender can generate is the cost of bandwidth.

Operating systems control access to resources by means of access control mechanisms. Traditional access control mechanisms consist of two parts, an authentication mechanism that determines who is making the request (e.g. the username and password used to log in) and an authorization mechanism that determines what they are allowed to do.

*Implicit*

In certain circumstances the authorization is implicit in being willing to perform the tasks necessary for authentication. For example providing a response to an email callback loop indicates that the sender is unlikely to be an automated process.

*Blacklists / Whitelists*

A whitelist is the opposite of a blacklist. Instead of specifying the parties who are not allowed to send messages a whitelist specifies the parties who are allowed to send messages.

*Revocable Credentials*

Cryptographic authentication schemes such as S/MIME or SSL use X.509 digital certificates as credentials. The X.509 specification allows for certificates to be revoked. If the criteria for revoking the credential include sending spam the possession of a valid credential is equivalent to membership of a whitelist.

*Sender Charges*

Spam effectively transfers the cost of advertising from the sender to the recipient. Many have argued that the way to eliminate spam is to change the economics of email so that the sender bears the costs of sending a message [Sender]. It is argued that a change as low as a small fraction of a cent would make spam uneconomic and drive spam senders out of business.

The chief practical difficulty with any such proposal is that the solution presupposes the deployment of an Internet infrastructure to support the charging system and a business incentive that would drive the ISPs who would end up being net contributors to adopt it.

While such infrastructures exist and are used for purposes such as inter-bank settlements the cost of deploying and maintaining such systems is ranked in the hundreds of millions. Even if a charge of a small fraction of a cent would be sufficient to eliminate spam it is unlikely that such an amount would be sufficient to pay for the infrastructure required to collect it. It is likely therefore that all ISPs would end up being net contributors.
It is highly unlikely that such a low charge would be sufficient to stop spam however. Costs ranging from $.50 to $5.00 appear to do little to discourage the indiscriminate sending of junk mail and unwanted telephone solicitations.

Closer examination of the spam problem reveals that it is the scarcity value of money that is useful in deterring spam rather than convertibility. A number of schemes such as HashCash [HashCash] propose mechanisms based on non-convertible tokens which are money like in that an artificial scarcity is introduced but avoid the numerous problems related to settlements and fraud that use of fungible money entails. While such schemes are certainly more practical than schemes based on actual money transfer the deployment challenges are still daunting.

In particular a large administrative infrastructure would be required to allocate appropriate numbers of tokens or token generating capability to each user or ISP. It is hard to see how such a scheme would not be very costly to maintain.

**LEGISLATION AND LITIGATION**

The purpose of criminal legislation in a democratic is to deter persons from engaging in the prohibited conduct. While it is unlikely that criminal legislation alone would eliminate spam such legislation would certainly create a deterrent for both the spam senders and the advertisers seeking their services.

The legislative process is very slow and time consuming. Legislatures are reluctant to pass any legislation until they are confident the implications are fully understood. Legislators will have to be convinced that any new legislation to address the problem of spam will bring benefits that significantly outweigh both the cost of enforcement and the political cost of committing the scarce resource of legislative time to the problem of spam rather than to other pressing problems.

**Prosecutions and Litigation under Existing Legislation**

As previously noted a substantial proportion of spam is illegal under existing law. The scams operated by the senders of ‘Nigerian letters’ are illegal under existing fraud law. Sending images of hard-core pornography to 7 year olds is illegal under existing law. Many of the quack medicines are offered in ways that violate state and federal laws.

Spam senders also violate the law in their methods. Use of a false sender address is an attempt to gain access to a computer system by fraud. A false sender address that impersonates another party is a form of identity theft and may also be actionable as defamation.

To date the majority of actions against spam senders have been civil. AOL has successfully brought cases against a number of spam senders including a $7 million judgment against CN Productions. Verizon has won unspecified damages and a permanent injunction against spam sender Alan Ralsky.

Although criminal actions are rare, they are not unknown. A New York court recently issued an injunction against a New York spam sender at the request of the New York Attorney General.
Spam Litigation
Spam has spawned two separate types of litigation, cases brought by ISPs and individuals who object to the use of their resources to send spam and cases brought by spam senders to prevent ISPs cutting off resources when spam senders have violated terms of use.

In June and September 1997 Cyber Promotions applied for and was granted preliminary injunctions against WorldCom and AGIS to prevent termination of Cyber Promotions’ service. Neither case progressed beyond the preliminary injunction whose principal purpose was simply to allow Cyber Promotions time to find an alternative means of access to the Internet. In both cases Cyber Promotions had obtained a written statement from the ISP stating that they were aware that Cyber Promotions was in the business of sending spam. As a result the ISPs could hardly claim that Cyber Promotions were in breach of their terms of service.

A relatively large number of civil cases have been brought against spam senders [SL]. These include:

In Re: Laurence A. Canter (1997, Tennessee Disciplinary Court)
Complaint: That a spam sent by Canter’s law firm Canter and Segal was sent contrary to various requirements of bar conduct.
Result: Canter was disbarred. It was found that the manner of sending the advertisement brought the legal profession into disrepute.

Claim: Bigfoot Partners claimed $1 million in damages and a permanent injunction preventing Cyber Promotions using Bigfoot to send spam.
Result: Permanent injunction issued under a consent order prohibiting the practices listed in the complaint with damages of $10,000 per day for non-compliance.

CompuServe v. Cyber Promotions (1997, Ohio Federal Court)
Claim: Cyber Promotions used forged mail headers in messages sent to CompuServe users causing CompuServe mail servers to become overloaded through attempts to deliver undeliverable mail.
Result: Permanent injunction issued under a consent order prohibiting the practices listed in the complaint.

Concentric Networks v. Cyber Promotions (1996, California Federal Court)
Claim: Cyber Promotions used forged mail headers with a Concentric Networks (CNC) return address, causing CNC mail servers to be overloaded with complaints about the spam.
Result: Permanent injunction issued by the court prohibiting the practices listed in the complaint.

Civil Claim: That the defendant ran a phony literary agency that charged writers fees for services that were not rendered.
Result: The result of the civil case was that the agency was ordered to stop its Internet publishing scheme, provide restitution to consumers, pay penalties and costs to the state and post a $100,000 bond to protect consumers in future business dealings.
Criminal Case: following the civil case the US Postal Inspector brought a criminal case in 1999. James Leonard and Ursula Sprachmann, the proprietors of the agency plead guilty to conspiracy to commit mail fraud and perjury. Leonard was sentenced to 8 months jail and 3 years probation. Sprachmann was sentenced to 3 years probation on grounds of ill health.
Parker v. C.N. Enterprises (1997, Texas)
Claim: Plaintiff alleged that the defendant sent spam that contained the plaintiff’s email address. As a result, the plaintiff received over 5000 irate complaints from the recipients of the spam.
Result: Permanent injunction issued by the court prohibiting the practices listed in the complaint, damages of $13,910 and attorney's fees of $5,000.

Seidl v. Greentree Mortgage (1997, Colorado)
Claim: Greentree Mortgage commissioned a spam to be sent by an independent contractor, Mark Van Keuren.
Counterclaim: The defendant attempted to bring a counterclaim against the plaintiff and his attorney alleging libel, interference with a business relationship and that the suit was an attempt to extort money from innocent advertisers who use the Internet.
Result: The Plaintiff's complaint was dismissed on the grounds that the spam had been sent by an independent contractor hired by Greentree and that Greentree was not liable for its actions. The counterclaim was also dismissed.

AOL v. CN Productions, Inc. (1998, 2001)
Claim: That CN Productions ‘bombarded’ AOL members with unsolicited advertisements contrary to AOL acceptable use policy.
Result 1: Damages of $1,819,863 and attorney's fees of $126,104 awarded and an injunction issued.
Result 2: Further award of $6,904,712 in respect of breach of the injunction.

Claim: Cyber Promotions claimed that it had a first amendment right to send spam to AOL members and that AOL enjoyed an effective monopoly such that AOL was bound to accept spam from Cyber Promotions under anti-trust laws.
Result: Court disagreed.

AOL v. Web Communications, Inc., et al.
Claim: That Web Communications sent AOL subscribers numerous pieces of unsolicited and unwelcome spam.
Result: Default judgment in favor of AOL, damages of $1,578,175 and issue of an injunction.

Other Cases
AOL currently lists a further 13 cases that are either pending or concluded with similar results [AOL].

The experience of litigation against spam senders is encouraging insofar as courts have demonstrated that they are willing to award large sums in damages against spam senders in the right circumstances. In particular AOL succeeded in several of its claims because the spam senders either knew or should have known that their activities were contrary to AOL's terms of service.
While Seidl v. Greentree did not establish any liability on the part of advertisers who employ spam senders the precedent set by other cases suggest that a suit against the spam sender itself might well have succeeded. Furthermore the Siedl case was an early decision under a state law that occurred before later judgments established that sending spam could constitute trespass and before the fact that many spam senders use illegal means to send their messages became common knowledge. It is possible and perhaps likely that future courts will revisit the finding under Siedl that a spam sender is an independent contractor and instead recognize that the advertiser and spam sender are co-conspirators.

Review of these cases suggests that the following measures may be taken to ensure that litigation against spam senders has a satisfactory result:

- ISPs should post an acceptable use policy that prohibits sending spam to email addresses supported by the ISP.
- A mechanism such as an acceptable use policy reporting mechanism or opt-out list might improve the willingness of courts to believe that spam senders knew or should have known and were careless of the fact that they were breaking the ISP's acceptable use policy.
- Anti-spam legislation would provide ISPs with a means of resisting attempts by spam sender to prevent ISPs enforcing their terms of service by obtaining temporary restraining orders.

**Anti-Spam Legislation**

In May 2002 the European Union issued a directive that directs member nations to introduce legislation that prohibits sending of unsolicited marketing messages unless the recipients ‘opt-in’.

A number of Anti-spam measures have been proposed in the US Congress that seek to regulate spam by requiring spam senders to respect ‘opt-out’ requests and prohibiting the use of forged sender addresses. Most proposals are based on existing legislation concerning junk faxes and telemarketing calls that have already been tested with constitutional challenges.

The chief objection to the ‘opt-out’ measures is that a recipient of a spam has no way to know the origin of a spam. It is therefore impossible for a spam recipient to know if opt-out requests are being respected or not.

While email spam senders have negligible support in Congress, the Direct Mail Association (DMA) that represents senders of junk mail and telemarketers has demonstrated a considerable degree of influence opposing ‘opt-in’ requirements to protect privacy. The spam senders compete with the DMA members and so the DMA is opposed to spam but will oppose any measure requiring opt-in which might set a precedent that may later be applied to its members.

One possible resolution of this problem would be to require spam senders to respect a one-way encrypted opt-out list of the type described earlier. Such a list would meet the need for verification without threatening the interests of the DMA and its members.

Another possible argument in favor of the opt-in approach in the US is that it is more likely to survive judicial review as being constitutional. In Nixon v. American Blast Fax the court found a blanket ban on junk fax advertisements to be unconstitutional. While this judgment contradicts the opinions of other courts and is currently under appeal, US jurisprudence has traditionally considered first amendment issues with considerable care. There can be no guarantee that the lower court’s finding that the government could have realized its objective without an outright ban by means of an opt-out database will not be sustained. It is therefore prudent as well as expedient for anti-spam legislation to take this course.
Pro-Spam Legislation

Not all the proposed anti-spam legislation being proposed is intended to solve the problem of spam. Some of the ‘anti-spam’ proposals being raised in private are really ‘pro-spam’ legislation intended to solve problems for senders of spam.

A common tactic used in the US to derrail popular legislation is to introduce legislation at the Federal level that proposes ‘harmonization’ of state laws that does so by pre-empting the existing state laws with weaker or sometimes completely ineffectual federal laws.

Another potential tactic is to attempt to force ISPs to accept all mail that does not meet some definition of spam. If that definition is sufficiently loosely worded, ISPs might become legally obliged to accept any email content, however objectionable provided only that it was sent from a member of a particular association.

It is important therefore that any spam legislation be carefully evaluated on its merits and not merely its title.

The Likelihood of Offshore Spam Havens

An objection made against proposals for anti-spam legislation is that the Internet is not a single jurisdiction and that no one country can therefore hope to control the Internet through legislation. When examined closely however the argument for ‘regulatory arbitrage’ appears to be a conviction born of commitment to ideology rather than objective analysis. Nation states have demonstrated a considerable capacity to control certain socially undesirable uses of the Internet through conventional police methods and close international co-operation. A significant number of prosecutions have been brought in a wide range of jurisdictions against writers of viruses, online casinos and pedophiles.

While spam senders might attempt to evade legislation by transferring their operations to accommodating jurisdictions such evasion is far from costless to the spam sender. Jurisdictions that provide flags of convenience for businesses engaged in dubious practices do so out of self-interest and not in the pursuit of a libertarian ideology. A spam sender that transfers operations to such a jurisdiction is certain to find their operations subject to a large number of service fees, local employment costs and in many cases bribes to ensure the continued compliance of officials. Spam is sent indiscriminately because the incremental cost of sending messages is low. Forcing spam senders to use jurisdictions of convenience would increase the cost of sending spam and introduce significant barriers to entry to new market entrants.

It is highly unlikely in any event that jurisdictions offering traditional offshore services such as tax havens, financial services or shipping would allow these already lucrative offerings to be threatened by the unwelcome attention that acting as a clearing house for spam would inevitably attract. Nor is it likely that the individuals attempting to profit from the business of sending spam would be anxious to take up actual residence in such jurisdictions. The only jurisdictions likely to tolerate spam sender operations on a large scale are countries where the entire apparatus of civil government has effectively collapsed. Endemic corruption and unstable government does not provide a fertile ground for any form of commerce requiring expensive high technology infrastructure.
DEPLOYMENT

As this paper shows, no proposal yet made provides a magic bullet that kills spam. Content inspection based approaches can be readily deployed but tend to lose their effectiveness as widespread adoption encourages spam senders to employ countermeasures. Legislative approaches can increase the costs of spam senders by forcing them to employ costly countermeasures such as moving offshore but are unlikely to eliminate spam altogether. Authentication based approaches provide a robust means of identifying messages that are not spam but are of limited utility unless widely adopted.

This analysis suggests that content inspection, legislation and authentication are complimentary approaches. Content inspection provides short-term mitigation of the effects of spam. Authentication provides a robust long-term solution. Legislation provides a means of slowing the rate of growth of spam so that the content inspection based approaches maintain their effectiveness long enough for the long-term authentication based solutions to be effective.

Changing Infrastructure

As the Internet grows larger, the difficulty of making changes to the infrastructure of the Internet increases. Contrary to the media myth, Internet time runs at the same pace as normal time.

One of the principal reasons for the success of the Internet is that it is built using genuinely open, freely available standards. Although many standards bodies define Internet related protocols, the Internet Engineering Task Force (IETF) defines the principal email protocols. A programmer who feels they can write a better Web browser can find the specifications that define the relevant protocols on the IETF web site. If the programmer feels that the protocols can be improved they can join an IETF Working Group and suggest improvements.

While the IETF has many virtues, its principal vice is that the pace of its deliberations is geared to the more leisurely pace of academia rather than the needs of Internet users. Major protocol revisions take decades rather than months or years.

The original SMTP protocol was defined in 1982 [SMTP]. Some changes were made in 1986 and extensions were defined in 1995. The first major revision of the original protocol took place in 2001 [SMTP2], almost two decades after the first proposal.

While there are currently plans to begin a research group in the IETF sister organization, the Internet Research Task Force (IRTF) there are no current plans for any IETF working group to examine revision of the mail infrastructure. It is unlikely that such a group could be started in less than a year and it is likely that any standardization work would take at least two years once started. Commercial implementation of the resulting standards would take a minimum of a year. The shortest time in which any standards effort may reasonably be expected to complete is thus four years.

Fortunately the IETF has a rather different role to most standards bodies. While most standards bodies develop a specification before the code to implement it is written the IETF favors the reverse approach. Instead of leading the development of the Internet the IETF documents it.
Protocol Changes to Facilitate Spam Measures
The previous sections have identified the need for mechanisms that allow:

- Unsolicited callback requests to be identified and suppressed
- Mail servers to communicate the results of server based authentication and filtering procedures to mail clients.
- Mail clients to cause mail servers to apply filtering at the server.
- Mail clients to disable server based filtering.
- Support for lightweight authentication mechanisms to be applied at the server level.

APIs for Spam Filters
The definition of a standard Application Program Interface (API) for filtering modules would greatly simplify deployment and allow development of spam filtering mechanisms to take place independently of email client development.

While a number of spam control frameworks exist, these tend to be ad hoc mechanisms tied to a specific platform or infrastructure.

Authentication Mechanisms
We identify a need for the following

- A means of advertising authentication policy through the DNS.
- A lightweight authentication mechanism that can be deployed with minimal overhead.
- Definition of a standard callback mechanism that allows a mail client to automatically detect callback loop requests that were initiated by the client and those that result from a message sent with a forged header.

Mailing List Management
As previously stated, support for mailing list software in SMTP is less than satisfactory. We propose the following set of protocol changes to remedy this situation.

- Mechanism identifying messages sent through a mailing list and the means by which the subscription can be cancelled.
- Mechanism that allows a mail server to determine that an email user solicited a message from a particular mailing list or other bulk sender.
- Authenticated subscription management mechanism.
- Mechanism for communicating the authenticated mailing list subscription mechanism to email clients.
- Mechanism for identifying automatically generated messages that should not be replied to under any circumstances
- Means of determining that an email client conforms to a consistent means of implementing the above.
**COMPREHENSIVE EMAIL MANAGEMENT**

The various mechanisms described in this draft may be brought together to provide a comprehensive email management solution as shown in Figure 1:

1. **Denial of Service Processor**
   When the mail server receives a request to send an email it first checks to see whether the email is being sent from an IP address that has attempted to perform a denial of service attack on the server by consulting the Denial of Service blacklist.

2. **Authentication Processor**
   The mail server performs the authentication procedures that are available to it, including verification of the source IP address, use of authenticated SSL and S/MIME authentication on the message itself.

3. **Authentication Policy Processor**
   If the sending domain has an authentication policy the mail server checks to see if the message meets that authentication policy. If the message passes the authentication policy or there is no authentication policy the message is passed to the authorization processor. Otherwise the message is rejected.

4. **Authorization Processor**
   The Authorization processor checks to see if the sender of the message is on the local whitelist of approved senders. If so the message is accepted, otherwise the message is passed to the Content Inspection module.

5. **Content Inspection Processor**
   The Content inspection module uses the heuristic approaches described earlier such as keyword filtering, header verification, blacklisting and Bayesian inference to determine whether the message is likely to be a wanted message or spam. The use of authentication techniques may be taken into account when determining the likelihood that the message is spam. If the message is identified as likely to be good it is passed to the user, otherwise the message is quarantined, either by placing the message in a ‘likely junk’ folder or by marking it in a manner that can be verified by the user’s mail client.
The Blacklists and Whitelist may contain information collected locally and information from external sources.

**Denial of Service Blacklist**
Denial of Service attacks typically target a single site or a small group of sites. It is likely therefore that in most cases the source of information for the Denial of Service Blacklist would be information collected at the site itself.

**Spam Sender Blacklists**
It is recommended that spam blacklists be used as one input to the content filtering decision-making process rather than to provide an accept/deny decision. In particular end users should not be deprived of wanted email messages because they are sent from a source address that has been listed to create ‘collateral damage’ as a means of establishing leverage to cause an ISP to change policy. In most cases neither the sender nor the receiver has direct influence over these policies and the annoyance caused to them by the use of these tactics is almost certain to be greater than that caused by the spam itself.

**Authorized Sender Whitelist**
The Authorized sender whitelist will typically be based on information configured locally from lists of known customers, suppliers and partners. In cases where robust authentication techniques such as digital certificates are used it may prove adequate to list exceptions to the whitelist.

The use of feedback from end-users is highly recommended to assist in the maintenance of the blacklists and whitelist and in the configuration of the content inspection processor. This feedback may employ Bayesian inference, least squares minimization or other optimization techniques.

**CONCLUSIONS - A PLAN FOR NO SPAM**

There are many techniques that address a part of the spam problem. No currently known technique provides a complete solution and it is unlikely that any technique will be found in the future that provides a complete and costless solution.

Even so, there are many techniques that in combination can provide an effective strategy for addressing the spam problem.

- **Do not send lists**, protected using one-way encryption provide an objective definition of a spam message.

- **Legislative initiatives** provide a means of increasing the costs of the spam senders and reducing the profitability of their enterprise.

- **Content Inspection** provides a means of identifying undesirable messages that can be deployed with immediate advantage to the user.

- **Authentication** provides a means of identifying desirable messages that allows the problem of false positives associated with content inspection to be reduced and with widespread deployment offers the possibility of a comprehensive solution.

- **Authentication Policy** provides a means of knowing that a message that does not meet the authentication policy specified by the domain name owner has been forged and should be discarded as spam.
• **Callback Loop** authentication is acceptable as a last resort when a message has been identified as likely spam. Its use as a first line of defense is not acceptable. A mechanism to prevent callback bombing is required.

• **Protocol improvements** provide support for the content inspection and authentication approaches and should be pursued aggressively.

Spam is a security problem. It is the lack of authentication and authorization in the email system that allows it to be abused for any purpose. The volumes of spam are rising at a rate that threatens the usefulness of email. Spam is therefore more than simply a problem for individuals or an opportunity for businesses that provide solutions, spam is a community problem and it is the Internet community as a whole that must find, implement and deploy solutions.

**LEGAL NOTICE**

The technology described in this document may be covered by claims made by patents issued or pending held by VeriSign Inc. or other parties. No rights to use such technology are granted in this document, nor is any form of warranty or other guarantee provided that such technology shall be licensed on particular terms or any terms whatsoever.

**REFERENCES**


[PHB] Phillip Hallam-Baker, Signature Velocity Indicator, to be published.


[BBC] BBC News, MPs’ e-mail filter system under review, February 7th, 2003 http://news.bbc.co.uk/1/hi/uk_politics/2737709.stm


