Network Working Group
Internet Draft
draft-crocker-spam-techconsider-02.txt
Expires: <12-03>

D. Crocker
Brandenburg
Vernon Schryver
Rhyolite Software
John Levine
Taughannock Networks
29 June 2003

Technical Considerations for Spam Control Mechanisms

SUMMARY

Internet mail has operated as an open and unfettered channel between originator and recipient. This invites some abuses, called spam, such as burdening recipients with unwanted commercial email. Spam has become an extremely serious problem, is getting much worse and is proving difficult (or impossible) to eliminate. The most practical goal is to bring spam under control; it will require an on-going, adaptive effort, with stochastic rather than complete results. This note discusses available points of control in the Internet mail architecture, considerations in using any of those points, and opportunities for creating Internet standards to aid in spam control efforts. It offers guidance about likely trade-offs, benefits and limitations.

CONTENTS

1. SPAM AND CONSENT

Internet mail has operated as an open and unfettered channel between originator and recipient. It has always suffered from some degree of abuse, in which originators impose on recipients inappropriately. In recent years, a version of this abuse has grown substantially. Called spam, its definition varies from "unsolicited commercial email" to "any email the recipient does not want". Often there are no technical differences between spam and "acceptable" email. Their format, content and even aggregate traffic patterns may be identical. Hence spam is a problem for fundamentally non-technical reasons, yet the Internet technical community must pursue technical responses to it. The lack of strong community consensus on a single, precise definition makes this particularly challenging.

For most working discussions, the term "Unsolicited Bulk Email" is sufficient. The salient point that it is a mass-mailing ensures that discussion covers the broadest concern of the user and provider communities. Mail that is not in some real sense "bulk" cannot flood networks or mailboxes. Essentially all mail that people object to, as "spam", is bulk. For example practically all objectionable advertising mail is also bulk, although modern techniques for targeted advertising can permit extensive content or address tailoring. "Bulk" is usually very difficult for an individual recipient to prove, but almost always easy to recognize in practice.

More detailed discussion must, of course, be precise in the definition of "unsolicited" and usually must distinguish between different types of mail, such as commercial, religious, political or personal.

The simplistic -- but entirely adequate -- summary of the role of spam on Internet mail is that it is an extremely serious problem, it is getting much worse, and it is proving difficult or impossible to eliminate. Spam is generated by a very wide range of clever sources and it always will be. Instead of thinking of spam as a disease that might be eliminated, it is more useful to think of it like crime, war and cockroaches.

It is not realistic to expect to eliminate any of these, no matter how much anyone might wish otherwise. Therefore the best we can hope to accomplish is to bring spam under reasonable control and that control will require an on-going, adaptive effort, with stochastic rather than complete results. That is, we need multiple, adaptive techniques. As spam changes, so must our mechanisms. Different mechanisms will be appropriate for different circumstances.

In other words, spam has become a permanent part of the Internet mail experience and efforts to control it may only reduce it to a tolerable level, rather than eliminate it. It is somewhat comforting to remember that an individual spam is not damaging. Rather the quantity of spam is what poses a threat. Hence there is flexibility in permitting spam control mechanisms to be imperfect.

This note discusses available points of control in the Internet mail architecture, considerations in using any of those points, and opportunities for creating Internet standards to aid in spam control efforts. It offers guidance about likely trade-offs, benefits and limitations.

The note does not offer an analysis of the types of spam or the types of attacks used in sending spam, nor is it intended to specify solutions. Similarly, the note does not discuss fine-grained details, such as the arguments associated with single opt-in mechanisms, versus double opt-in. These points are important to the engineering of particular solutions, but only as refinements after the larger architectural and system control choices are made.

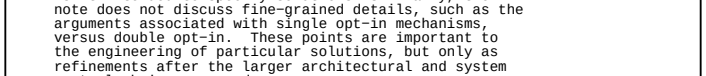
Note: This document is intended to evolve, based on comments from the Anti-Spam Research Group (ASRG) mailing list. It is certain that the current draft is incomplete and entirely possible that it is inaccurate. Hence, comments are eagerly sought, preferably in the form of suggested text changes, and preferably on the ASRG mailing list, at <mailto:asrg@ietf.org>

STD OPP [0] Throughout this document, opportunities for technical standards are cited. These represent an attempt to provide a complete list of such possibilities, rather than to offer recommendations. These will be in entries of this form, with the label "STD OPP".

2. ARCHITECTURAL REFERENCE

2.1. Email Control Points

Email transmission sequences can touch many systems, between the originator and the recipient. However for most discussions about control, only five major components are important:



UA.o: The originator's user agent, operated by the user and under their direct control

MTA.o: The mail transfer agent service associated with the originator's environment, possibly operated by the sender and possibly operated under separate control, such as by their employer.

MTA.i: The mail transfer agent service operated by an independent third-party, such as an Internet Service Provider (ISP)

MTA.r: The mail transfer agent service associated with the recipient's environment

UA.r: The recipient's user agent

In many organizations, the MTA service is multi-stage, such as including a department MTA and an Internet "firewall" MTA. This distinction is of fundamental importance for making software and operations decisions, but it does not have a significant impact on a discussion about points of control. Points of control are primarily affected by crossing administrative boundaries. Therefore the distinction between originator's environment, recipient's environment and any independent third parties is essential to this larger examination. These are separate, independent administrative environments and are subject to different policies. In particular, note that a discussion about using control points hinges on the scope of the control to be exercised.

Besides constituting a major burden to recipients, the volume of spam traffic has become a serious problem for transit services. Hence a precept in controlling spam is to seek control as close to the source as possible. The fewer downstream resources consumed by spam, the better. Of course, the ideal would be a mechanism in UA.o that would prevent spam from being sent in the first place. Indeed, legal remedies seek to affect a sender's motivations, so that they will not send the spam at all.

Unfortunately there is no opportunity for software control of spam in UA.o , because the software is under the control of the originator. If they wish to bypass any control mechanisms in UA.o , they will find a way. Of course, some services have UA.o under administrative control from the software's user. This affords a software choice, placing controls in that module, but does not permit the more general architectural specification of controls there, because the separate administrative control cannot be relied on.

The next opportunity is MTA.o. Often this service is operated by a group independent of the originator.

Wherever the detection mechanism is placed, the critical challenge is to identify spam in real time, if its relaying and delivery are to be stopped. The other avenue is post-hoc removal of the right to make further use of the MTA service. This may have strong utility for spammers attempting to operate within acceptable social bounds. It will have no effect upon spammers who avoid accountability.

2.2. Terminology

When determining whether a message qualifies as spam, different types of email attributes can be considered, different types of analyses can be performed on them. Equally the results of the analyses can be used in different ways, for preventing, detecting or following up occurrences of spam.

2.2.1. Evaluation Focus

When discussing both the attributes of spam and the mechanisms for controlling it, the major distinction for evaluation is between:

Originator: Evaluate the trustworthiness of creator of the content. Will the originator create spam?

Content: Evaluate the message content, itself. Does the content contain spam?

Destination: Evaluate whether special destinations were specified, such as honeypots

Traffic Evaluate the aggregate posting behavior, to determine whether multiple, related postings qualify as "bulk"

Validating the originator can often be done with excellent reliability. However current common practises for author authentication have resisted wide-scale adoption and this approach only protects against spam indirectly. The creator might choose to violate the criteria used to assess them. When validation of the originator is based on the contents, this certifies authorship, but does not certify any other characteristic of the content.

By contrast evaluating content is direct -- either it is spam or it is not -- but it is impossible to do the evaluation perfectly. For example, legitimate subscription-based bulk mail is technically identical to spam, in every regard, except that it is solicited or desired by its recipients. Simplistic content evaluation criteria have a high rate of false positives and are easily bypassed by spammers, leading to a high rate of false negatives. Complex criteria are difficult to create and maintain. They, too, are likely to have a high rate of false assessments, eventually, unless maintenance of the analysis rules is diligent.

2.2.2. Originator Focus

Evaluation of the originator sub-divides between:

Author: Evaluate whether the person creating the content is likely to create spam.

System: Evaluate whether the system that is sending email on a person's behalf is likely to permit spam to be sent.

Evaluating the person (or organization) creating the message is direct, albeit still carrying the caveats noted above. Evaluating the system is indirect, but presumes that the system enforces quality assurance policies on the email sent from it.

A larger problem with evaluating the originator of mail is that Internet mail necessarily and desirably involves receiving mail from strangers. Mailboxes that are closed to mail from strangers do not have a spam problem. On the other hand, it is impossible to know whether copies of a message from a stranger are also being sent to 30,000,000 of your closest friends. Contrary to often-expressed hopes, a third party that is also a stranger cannot attest to the virtue of a mail sender. A letter of introduction from a stranger does not make the bearer other than a stranger.

If the history of spam is any guide, organizations such as Internet service providers and public key infrastructure (PKI) providers cannot be expected to ensure that their customers do not send spam. Even with the best of intentions, they will always be willing to open new accounts to strangers. The most that can be expected is that they will punish their spamming customers such as by imposing substantial fees or filing lawsuits. It should be noted that the "punishment" of terminating their account often is meaningless, because many spammers create one-time accounts.

2.2.3. Detection

Qualification performs tests against one or more criteria. Test results are:

Positive: Message matches the test criteria.

Negative: Message fails to match the test criteria.

When the tests are heuristic or statistical, some portion of the results will be incorrect.

Incorrect results are classed as:

False Positive (FP): The filter classified a non-spam message as spam. That is, the message matches the test criteria, but the criteria are too aggressive.

False Negative (FN): The filter classifies a spam message as non-spam. That is, the message fails to match the test criteria, but the criteria are not sufficiently strong.

2.2.4. Disposition

Filters are used for two, basic and complementary purposes:

Acceptance: Approves mail for delivery.

Rejection: Withholds or refuses permission for delivery.

Implementations of filter mechanisms may provide for a range of choices, rather than simple acceptance or rejection.

Note that rules for acceptance are equally subject to error. However Acceptance rules are usually for simple, explicit rules rather than heuristics, so that FP and FN results are not usually a concern. Hence discussion of FP and FN are usually for Rejection rules.

2.2.5. Simple Filtering

The combined range of capabilities for detection and disposition of email can produce complex, heuristic behaviors. For better efficiency and predictability, such mechanisms usually permit specification of explicit lists of criteria and values that, when present in the message, prompt direct disposition. The simplest method of testing is to have explicit lists of simple identifier criteria, such as From address or standard text in the Subject header.

Pre-assessed values are entered into:

Whitelist: Automatic Acceptance

Blacklist: Automatic Rejection

One approach to maintaining Whitelists and Blacklists is to make explicit entries into them, manually. This is often what a spam control service will offer to its subscribers. Most such services are for blacklisting known sources of spam.

A difficulty with these listing services is the set of criteria used for adding and removing senders or sites. These policies usually need to be explicit, objective, documented and consistently applied. Even then, blacklist operators are attractive targets for threats of lawsuits claiming inappropriate listing, interference in business or trade, etc.

3. APPROACHES TO CONTROLLING SPAM

3.1. Administrative and Legal Mechanisms

Both government law and service provider contracts can be used for defining unacceptable behavior, requiring preventive measures, and providing for remedies when there are violations.

There are two major problems with this administrative approach to the control of spam. One is that the sender often cannot be readily identified by the recipient of spam. There are many opportunities for practically anonymous posting of email, including Internet cafes, transient access services and free email services. The second problem is that the sender of spam may not be in the jurisdiction seeking to exercise control or a jurisdiction responsive to the recipient's jurisdiction. The Internet is global. Unlike postal bulk mail, the cost of sending spam over the Internet does not change as the mail crosses jurisdictional boundaries.

Hence it seems likely that use of administrative procedures can be effective for controlling "responsible" spam -- that is, spam sent by organizations operating as accountable social participants. Perhaps they indulge in overly aggressive policies, but they still desire to be socially tolerable. The large number of "rogue" spammers is not similarly burdened.

However, most "rogue" spammers are trying to sell a product or service. There have been notable successes against spammers by the U.S. federal government ""following the money." ." However the government staff for these activities note their lack of resources and the extensive effort to achieve the result.

3.2. Infrastructure and Operations

Enhancement of underlying Internet services might reduce the effectiveness of some spam transmission mechanisms. For example many spammers prefer to send to domain name service MX secondaries because secondaries are often not as well filtered as MX primaries. Because of MX secondaries lack a coordination protocol, the best advice for all but the largest sites is to stop using MX secondaries. This advice sounds radical, but MX secondaries are no longer needed to compensate for intermittently connected or sending MTAs. Today MX secondaries are generally needed only for ""load balancing" " when there is more incoming mail than can be handled by a single SMTP server.

STD OPP [1] An MX secondary coordination protocol could coordinate standardized filtering rules, white- and blacklist entries and other spam control data among MX servers.

[2] Best Current Practises (BCP) documentation of preferred MTA operation for spam control, beyond that documented in RFC 2505. For example, it is better to reject spam by rejecting the SMTP transaction with a 5yz status code than to accept the transaction and later send a delivery failure notification.
[3] BCPs for operational conventions relevant to other other spam control services, such as DNS blacklists

Postal mail imposes a fee on the sender for each message that is sent. Such a fee makes the cost of sending significant, and proportional to the amount sent. In contrast, current Internet mail is very nearly free to the sender. Hence there is interest in exploring "sender pays" email.

One form of sender-pays is identical to postal stamping. Another entails imposes post-hoc actions on the sender, taking the fee for their posting only if the recipient indicates they were unhappy to receive it. For both models, it is not clear that it is possible to retroactively fit the necessary mechanisms to Internet mail. Its complete absence from the current service and the existence of anonymous and free email services may provide too much operational inertia. It is also not clear who should receive the fees or how they should be disbursed.

3.3. Filtering

The technical mechanism for real-time detection and handling of spam is a filter, placed at MTA.o, MTA.i, MTA.r and/or UA.r. A filter has two functions: detection and action. Action is usually either adding a special label to the message or disposing of it.

3.3.1. Traffic Analysis

Spam is often referred to as "unsolicited bulk mail" to highlight that senders typically post very large amounts quickly. Opt-in (subscription) email also demonstrates this traffic pattern. Still there is benefit in measuring aggregate email behavior.

STD OPP [4] Traffic reporting protocol, to permit collaboration among independent administrations.

3.3.2. Content Analysis

Filters look for message attributes, such as strings of text in the headers or content of the message being inspected. Other attributes include the address or domain name of the originating system or the occurrence of the same message content in multiple messages at the same time. Simple filters look for specific strings. A more powerful approach looks for multiple sets of strings, assigning a positive or negative score to each occurrence; it then labels spam according to its total score.

Rule creation is done manually, or by a service, or by analysis of a collection of messages. For example one type of service observes email traffic at many Internet locations and receives reports as recipients see new types of spam. The service then propagates new rules to its subscribers. One example of an analytic approach performs empirical rule creation, using statistical techniques, such as Bayesian, to discern string occurrences in known spam, versus mail that is known not to be spam.

As rules become common, spammers adapt their messages to bypass filters, so that existing rules quickly become less effective. Hence a long-term filter must

use rules that are continually modified. Empirical rules generation must be repeated, or must operate continuously, analyze all incoming mail.

Manual rule maintenance is simply not practical for typical users; the effort is far too great and the nature of rules such as ""regular expressions" " are too arcane. A concern about services is that they are inherently post-hoc. They are always updating the rule-set after an "attack" commences, so that some spam is certain to reach some recipients; however the view that a small amount of spam is not dangerous mitigates this concern. Lastly, methods using automated analysis rely on heuristics, or guesses. They are certain to have some percentage of "false negatives" (FN) that permit real spam to reach the recipients, and some percentage of "false positives" (FP) that incorrectly label legitimate mail as spam.

Any effective, long term filtering mechanism must have automatic or semi-automatic rule creation and must upgrade the set of rules continuously or periodically.

STD OPP	[5] Format and exchange mechanisms, to permit sharing rules, rule templates, white/black list entries.
	[6] Sample message labeling and exchange, to permit submission of candidate content to remote service.
	[7] Hash-based identifier of content

3.3.3. Tagging

Message originators and transit handlers can facilitate filtering efforts by adding standardized information, or tags. The most serious difficulty with any scheme that relies on tagging is its relationship to the larger body of email that is untagged. What does it mean when the tag is not present? Is presence of the tag a certain indicator of the intended information? Is there benefit in falsely labeling the content? Does the scheme contain a means of preventing this spoofing?

If tagging uses a simple string label, such as "ADV" to indicate that the contents contain advertising, how is this useful when most email is not labeled or is labeled incorrectly? This is like postal-based mass marketing that has an envelope marked "personal and confidential" but is neither.

Non-forgeable tagging uses cryptographic techniques. If the tagging identifies the sender, then the recipient must have access to the cryptographic identifier. If the tag is independent of the content -- that is, it identifies and authenticates the sender, but uses a scheme that does not integrate the specific content of the contained message -- then what is to prevent re-using the identification inappropriately?

STD OPP	[8] Standardized tags, according to different criteria

3.3.4. Filter Rules

The simplest model for a filtering test is to have entries containing a single, simple attribute, such as sender email address or source system IP address or domain name.

For assessments based on the identity of the sender, rather than the content of the message, another concern is validation of the key attribute used for identification. What if the value for that attribute is set falsely? For example, what if email was not send by the address listed in the From field?

STD OPP	[9] Common metrics about message sender behaviors, to allow calculation of their "reputation".
	[10] Format and access to filter logs, such as among MX secondaries. Spammers sometimes spread their mail among the MX secondaries for a domain. Correlating typical SMTP log files merely by time and data is onerous.
	[11] Control protocol between recipient and filtering service server, to permit specifying policies and specific rules.
	[12] Modify SMTP delivery status notifications to avoid flooding innocent mailboxes because of forged senders. [Needs clarification. /ed]
	[13] Codify best current practices of filters to minimize sending DSN. Delivery status notifications announcing the rejection of spam often go to innocent third parties when the sending address of the spam has been forged. Rejecting the message during the SMTP transaction often, but not always, prevents this ""collateral damage." ." [This may duplicate a previous opportunity. /ed]
	[14] Codify DSN and SMTP status message wording, such as saying that rejections resulting from filtering should include a URL for an extended explanation. [Needs clarification. /ed]
	[15] Replace SMTP.

The idea of replacing SMTP is appealing because it permits thinking in terms of creating an infrastructure that has accountability and restrictions built in. Unfortunately an installed base the size of the Internet is not likely to make such a change anytime soon. It seems far more likely that successful spam control mechanisms will be introduced as increments to the existing Internet mail service.

Moreover, the feature of SMTP that is most responsible for spam is the ability to receive mail from strangers. Without this feature, there would be no flood of spam, but many of the most valuable Internet commercial and individual activities would also be impossible. Replacing SMTP with a protocol that allows strangers to send each other mail would not stop spam any more than SMTP-AUTH stopped spam, contrary to insistent claims to the contrary, before SMTP-AUTH became widely available and used.

3.4. Negotiation

In addition to real-time analysis, a recipient may engage in an explicit negotiation with the sender, to validate them.

When this is performed at the time of message receipt, it is called a "Challenge-Response"(CR) mechanism. This mechanism might use regular email exchange, or other media supporting interaction. An example of a mechanism could have the recipient MTA contact the putative sender's host, as addressed by the DNS MX record associated with the Mail-From domain name. It could send that domain a hash of the received message and ask, "Did you really send this"? The effect is essentially the same as a cryptographic message authentication, but implemented through a callback mechanism, rather than being carried with the message content.

CR introduces delay in message receipt and creates at least one additional email round-trip exchange for every new sender/recipient pair. This is a substantial burden both on participants and on the transit service. Senders often refuse to respond to the challenge, so that the mechanism dissuades senders from all but the most urgent communications. In addition, the delay imposed by CR can render time-sensitive messages useless.

STD OPP	[16] Validation protocol (such as "challenge/response") between the recipient's and the sender system

4. EVALUATING TECHNICAL APPROACHES

The complexity of Internet mail service and the nature of spam make it difficult evaluate proposals for control mechanisms. In this section, the key technical factors affecting viability are examined.

4.1. Adoption

A critical barrier to the success of a new mechanism is the effort it takes to begin using it. It is essential to look carefully at the adoption process.

1) Adoption Effort	What is the effort for a new participant to start using the proposed mechanism? This includes installation, learning to use it and performing initial operations. This is also called the "barrier to entry".
2) Threshold to benefit	What is required before users get some benefit from the mechanism? Primarily, this looks for the number of users who must adopt the mechanism before the adopters gain utility from it.

A key construct to examination of adoption and benefit is "core-vs-edge". Generally, adoption at the edge of a system is easier and quicker than adoption in the core. If a mechanism affects the core (infrastructure) then it usually must be adopted by most or all of the infrastructure before it provides meaningful utility. In something the scale of the Internet, it can take decades to reach that level of adoption, if it ever does.

Remember that the Internet comprises a massive number of independent administrations, each with their own politics and funding. What is important and feasible to one might be neither to another. If the latter administration is in the handling path for a message, then it will not have implemented the necessary control mechanism. Worse, it well might not be possible to change this. For example a proposal that requires a brand new mail service is not likely to gain much traction.

By contrast, some "edge" mechanisms provide utility to the first one, two or three adopters who interact with each other. No one else is needed for the adopters to gain some benefit. Each additional adopter makes the total system incrementally more useful. For example a filter can be useful to the first recipient to adopt it. A consent mechanism can be useful to the first two or three adopters, depending upon the design of the mechanism.

3) Impact on Participants	What is the impact on the senders and receivers who adopt the proposal? Senders and receivers currently have certain styles of operation. How are those styles changed?
4) Impact on Others	What is the impact on the senders and receivers who do *not* adopt the proposal? What effect does it have on legitimate users of email? What effect does it have on spammers? Is the nature of Internet mail changed for everyone, including non-adopters?

For example, a challenge-response system is irritating for the person being challenged, and it imposes extra delay on the desired communication. If the originator and the recipient both access the Internet only occasionally (such as through dial-up when mobile) a challenge-response model can impose days of delay. For some communications, this can be disastrous.

4.2. Burden

The purpose of spam control is to cause some email to fail to reach its intended destination. This is, of course, directly at odds with the constructive goal of email. Hence spam control alters the basic model of email service.

Effective mechanisms must place some kind of burden on senders and receivers. Hence a challenge for spam control mechanisms is to require enough of a burden to be effective, but not so much that it makes email unacceptably painful to use.

5) Ongoing effort	UsageOnce a user has chosen to make the change to adopt a mechanism, how much effort does it take to use it regularly? After the effort to adopt the mechanism, how does it affect regular email use in an ongoing basis?
6)Balance of burdens	What is the nature and distribution of the burdens placed on senders and receivers who are affected by the proposed mechanism? Who must work harder to use the proposed mechanism?

4.3. Scaling

"Adoption" is the process of placing a new mechanism into an operational environment. Scaling looks at the effect of having very large numbers of participants use

that mechanism.

7) Use by Full Internet — What happens if everyone on the Internet adopts the proposed mechanism? How is the fabric Internet mail affected when there is very large−scale use?

8) Growth of Internet — What if the Internet grows by a factor of 1000? How is the fabric affected when there is much larger−scale use?

Remember that "everyone" is approximately 100 million users at the time of this writing. It will to grow to 10 billion, if we expect the Internet to be useful for some decades. And it is likely there will be more email users/accounts than there are people on the planet, given that individuals and organizations occupy multiple roles.

So, what will it be like for 100 million or 10 billion users to employ the proposed mechanism? Are there technology or operations "choke points" in the proposed mechanism?

9) Efficiency — Will the proposed mechanism be sufficiently efficient? Is Internet mail delivered in a timely fashion? Is the burden on processing and storage acceptable?

10) Cost — Will the proposed mechanism be sufficiently inexpensive?

11) Reliability — Will the proposed mechanism be sufficiently reliable? Is non−spam email more likely to be delivered correctly? Less likely?

There is another side to the scaling question:

12) Internet Impact — How much of the Internet will be affected by a proposal, if the proposal is adopted?

13) Spam Impact — How much spam will be controlled by the proposed mechanism?

If a proposal requires substantial effort to adopt and use, but will affect only a small percentage of spam, the efficacy of that proposed mechanism is very much in question. One example of this concern might be legal scope, given that spam is global and there is no global law enforcement.

4.4. Robustness

After a technique is adopted, spammers will adjust their techniques, attempting to work around the technique. For example, when people started using header filters, spammers started using bland deceptive subject lines, which mean that when spam gets past the filters, people are more likely to open messages and see porn pix. If whitelists become common, it is possible to envision spammers attempting to forge From addresses that are likely to be on the recipient's whitelist.

14) Circumvention — How difficult will it be for spammers to change their mail to bypass the proposed scheme? How are circumvention efforts likely to affect non−spam mail?

4.5. Scenarios

Almost any proposal will make sense for a particular scenario that is sufficiently constrained. The real test is how the proposal works for other, likely scenarios.

Make sure the proposal considers these likely cases carefully. There are many others. Here are some typical scenarios that often discriminate among proposals for changes to email:

15) Personal post/Reply — For two individuals wishing to exchange periodic email, how does the proposed mechanism work for initial contact? How does it work for ongoing contact?

16) Mailing List — Mailing lists are particularly interesting because special software performs a multi−cast redistribution of a message. Still, the From field of the message is from the originator, rather than the mailing list. How does the mechanism perform in this sort of mediated distribution? Does a recipient "reply" still work properly?

17) Inter−Enterprise — Two or more organizations often form special, cross−group teams to collaborate on projects. What is required to configure the proposed mechanism to support such teams? What is required to maintain the mechanism, as membership in the team changes? How are intra−team communications affected?

5. SECURITY CONSIDERATIONS

This note discusses types of mechanisms for evaluating and filtering email. As such, it covers topics with extremely sensitive security concerns. However it does not propose any standards and therefore does not have any direct security effects.

5.1. Privacy Considerations

Many spam control techniques affect the privacy of mail senders, receivers, or both. Bulk counting techniques can disclose the contents of mail, in systems that exchange message bodies, and can permit traffic analysis, in systems that use non−text message hashes or digests. Content filters can reveal message contents if filtered messages are examined by network personnel to check for false positives or negatives. Aggressive filtering can cause bounces and double bounces that send messages into postmaster mailboxes, disclosing content. If senders or recipients must appeal to have filtering criteria changed to avoid false positives, informal traffic analysis is possible based on the filtering terms in question.

Sender tagging and other techniques intended to deter address forgery make it more difficult to send anonymous or pseudonymous mail. E−postage schemes can identify senders unless the scheme allows users to buy and redeem stamps anonymously.

Several popular spam control systems involve routing incoming mail through the mail systems of third parties that are responsible for filtering mail. This exposes their contents to those parties.

These privacy risks can in principle be known to mail receivers, although operators of mail systems often fail to inform users of the anti−spam tools and third party services through which their mail passes. Mail senders often cannot know even in principle about these risks to their privacy.

6. APPENDIX

6.1. Spam Control Proposal Evaluation Checklist

1) Adoption Effort

2) Threshold to benefit

3) Impact on Participants

4) Impact on Others

5) Ongoing Usage effort

6) Balance of burdens

7) Use by Full Internet

8) Growth of Internet

9) Efficiency

10)Cost

11)Reliability

12)Internet Impact

13)Spam Impact

14)Circumvention

15)Personal post/Reply

16)Mailing List

17)Inter−Enterprise

6.2. Acknowledgements

This note is motivate by discussions on the Anti−Spam Research Group (ASRG) mailing list and draws a number of points from discussion there. The sub−section "Burden" was taken from a posting by Dave Hendricks.

6.3. Authors' Addresses

Dave Crocker
Brandenburg InternetWorking
675 Spruce Drive
Sunnyvale, CA 94086 USA
Tel: +1.408.246.8253
dcrocker@brandenburg.com

Vernon Schryver
Rhyolite Software
2482 Lee Hill Drive
Boulder, Colorado 80302
vjs@rhyolite.com

John R. Levine
Taughannock Networks
PO Box 727
Trumansburg NY 14886
Tel: +1.607.330.5711
johnl@iecctaugh.com

6.4. Full Copyright Statement