Task Force on Spam

Recommended Best Practices for Internet Service Providers and Other Network Operators

Working Group on Network and Technology Management

May 2005

Contents

Preface

The release of *An Anti-Spam Action Plan for Canada* in May 2004, and the creation of Canada's Task Force on Spam launched a concerted national effort to deal with an increasingly serious problem. In recognition of the importance of technical solutions to this problem, the Task Force established, among other working groups, a Working Group on Network and Technology Management.

The creation of this working group represents the first-ever collaborative and concerted effort involving a broad range of organizations, including most of the country's largest and smallest broadband and dial-up Internet service providers (ISPs), other network operators, large enterprise users, software developers, anti-spam advocates, and government. Gathering these stakeholders together to facilitate the free and frank discussions they have had, is, in itself, a tremendous accomplishment.

The Working Group on Network and Technology Management has developed a series of recommended technical best practices intended to help reduce spam in Canada. The Working Group's mandate represents a continuation of the efforts and progress that have been under way for some time, in Canada and internationally. The Working Group has, however, advanced this work to establish the first truly national consensus on technical measures to combat spam. Through these best practices, Canada has a model it can share internationally in the global fight against spam.

While the best practices are voluntary, the Working Group is pleased to note that a number of Canadian ISPs and network operators across the country have already started to implement some or all of these recommendations to protect the best interests of their customers and their networks. Moreover, these ISPs are increasingly requiring other ISPs and network operators to implement the best practices as a condition for accepting their email traffic. As such, the best practices will create a significant incentive for Canadian Internet industry stakeholders to harmonize their technical anti-spam practices throughout ever-evolving technologies.

Background

The Internet is not what it was 10 years ago when it became a consumer and business phenomenon. In 1995, unsolicited commercial email (spam) was virtually unheard of. Internet users up to that time, who had mostly been technical users, respected the medium as a productivity and communication tool. Network abuse by users was minimal, and acceptable use policies were largely respected.

Ten years later, we find ourselves facing a barrage of disinformation, misinformation, and wasted bits and bytes. About 66 percent of email messages are considered spam. The capacities of our physical networks and our network staff are tested daily in the seemingly never-ending fight to retain the integrity of our service.

The past year has seen a flurry of anti-spam activism on many fronts, and it has not been limited to Internet service providers (ISPs) or the network management industry. The Internet provider associations of almost every nation are tackling the problem. As well, alongside their more traditional roles, organizations such as the United Nations and the Organisation for Economic Co-operation and Development have struck committees to deal with spam.

Closer to home, the Internet industries in the United States and Canada have been holding a variety of discussions on combating spam. In the U.S., the Anti-Spam Technical Alliance, an organization that also includes representatives from several large Canadian ISPs, has developed and published a list of recommended best practices promoting network management practices that can help in the fight against spam.

Task Force on Spam

On May 11, 2004, the Minister of Industry announced the establishment of a Canadian Task Force on Spam to oversee the implementation of a comprehensive action plan to reduce the volume of unsolicited commercial email.

Chaired by Industry Canada, the Task Force has taken an open, consultative approach bringing together experts and key stakeholders representing Canadian ISPs and other network operators, business enterprises that use email to conduct legitimate commercial activities, consumer groups, and the legal profession.

To do its work, the Canadian Task Force on Spam struck working groups, one of which is the Working Group on Network and Technology Management. This Working Group includes representatives of most of the country's largest broadband and dial-up ISPs and other network operators (which the Working Group defines as including large enterprise users, such as universities and government departments), as well as software developers and anti-spam advocates.

The Working Group has been reviewing work conducted by formal and informal ISP and network operator groups, and has developed a list of best practices. These best practices can be used by ISPs and other network operators to help curb the abuse of networks, both from within, by customers, and externally, by spammers directing email toward customers.

Scope of Work

In August 2004, the Working Group on Network and Technology Management started developing a number of technical best practices that would contribute to the reduction of email spam. The Working Group's mandate represents a continuation of the efforts and progress that have been under way for some time, in Canada and internationally, including the work of the Anti-Spam Technical Alliance (ASTA) and the Messaging Anti-Abuse Working Group (MAAWG), and the efforts of various industry associations. A number of different ISPs, other network operators, technical groups and forums have been working collaboratively for many months to share best practices for reducing spam.

The Working Group on Network and Technology Management did not try to redo work that had already been done. Rather, it sought to bring the various industry groups together to share the results of work already under way, and to encourage the broad adoption of best practices among ISPs, other network operators and large enterprise users.

The Working Group emphasizes that the widespread adoption of these best practice*s* will not, in and of themselves, constitute a comprehensive solution to spam. They are, however, part of a broader, multi-prong strategy for addressing the problem of spam.

Intent

The Working Group's recommendations for best industry practices to combat spam are voluntary. The actual time frames for their implementation may vary, depending on the technical configurations of particular providers'/operators' networks, and their specific business needs and challenges. In some cases, alternative solutions may achieve the same objectives outlined in the recommendations. The selection of solutions is at the discretion of the provider/operator.

The Working Group supports all efforts to combat spam. Flexibility in the implementation of the recommended best practices is the key to achieving their broad and meaningful adoption by service providers of all sizes. Because of the technical nature of these recommendations, and the rapid pace of technological change, the Working Group is strongly of the view that these recommended best practices should not be codified as mandatory requirements.

Recommended Best Practices and Rationales

Following are the recommended anti-spam best practices for Canadian Internet service providers and other network operators, as well as a rationale for each recommendation.

1. **All Canadian registrants and hosts of domain names should publish Sender Policy Framework (SPF) information in their respective domain name server zone files as soon as possible.**

The purpose of email-sender authentication is to reduce domain-name spoofing in email, thereby reducing the incidence of spamming and phishing attempts.

Methods of sender authentication are continuing to be evaluated by the Internet Engineering Task Force (IETF). At this point in time, the SPF classic (SPFv1) proposal is the most technically mature and widely deployed sender-authentication scheme.

This recommendation does not preclude the use of other methods to authenticate email messages (e.g. sender ID, domain keys, SPF, identified Internet mail, etc.). Standards will continue to develop within the industry.

2. **ISPs and other network operators should limit, by default, the use of port 25 by end-users. If necessary, the ability to send or receive mail over port 25 should be restricted to hosts on the provider's network. Use of port 25 by end-users should be permitted on an as-needed basis, or as set out in the provider's end-user agreement / terms of service.**

Most ISPs and other network operators agree that there is no practical reason for dial-up/dynamic IP-address ranges to have email servers at the customer end.

There are a variety of ways to avoid this. Through their own network management, ISPs and other network operators can block the use of port 25 on an egress basis.

It has been the experience of members of the Working Group that blocking port 25 affects very few users, and that these users can usually be accommodated in other ways.

The benefits of blocking port 25 are frequently dramatic — some ISPs have seen a 95-percent drop in virus emissions, a 98-percent drop in abuse reports, a reduction in internal viruses / compromised machines used to send spam and attendant cost savings in abuse-related network management.

3. **ISPs and other network operators should block email file attachments with specific extensions known to carry infections, or should filter email file attachments based on content properties.**

Many viruses and worms are carried by file attachments. Blocking email containing problematic attachments would have little impact on users. The most common file extensions carrying a payload are: .pif, .scr, .exe and .vbs.

Many ISPs and other network operators should filter attachments based on their properties (i.e. infections) versus extension names. This is a matter of resource availability. Since some business or technical users may have legitimate reasons for sending .exe or .vbs files, filtering for content may be more efficient than filtering for extension names.

4. **ISPs and other network operators should actively monitor the volume of inbound and outbound email traffic to determine unusual network activity and the source of such activity, and should respond appropriately.**

Monitoring and possibly rate-limiting the amount of email that can be sent from a particular user would be useful in discouraging spammers from using provider networks as their launching points. It would also provide an early indication of the possible infection of user machines.

Some providers currently do a limited amount of rate limiting. Techniques will vary depending on the email server in use.

5. **ISPs and other network operators should establish and consistently maintain effective and timely processes to allow compromised network elements to be managed and eliminated as sources of spam.**

Using viruses, worms and malicious software, hackers and spammers have intentionally deposited millions of "back-door" open relays and proxies on the personal computers of unsuspecting users. The spammer community uses this network of compromised devices to generate billions of unsolicited email messages. In addition, hackers have used this network of devices to mount distributed denial of service (DDoS) attacks on websites, register fraudulent accounts and lay the groundwork for future anonymous hacking activities.

There are a number of methods that can be used to address compromised devices, from suspending client accounts to isolation or quarantine from the network.

6. **ISPs and other network operators should establish appropriate intercompany processes for reacting to other network operators' incident reports.**

The Working Group on Network and Technology Management is developing a list of ISPs and other operator contacts. It would be beneficial for operators to have common response expectations when reporting incidents of significant network abuse to other network operators. Escalation processes within companies would remain a proprietary process, but initial intercompany communications need a common "estimated time to recovery."

7. **ISPs, other network operators and enterprise email providers should communicate their security policies and procedures to their subscribers.**

This is to ensure that subscribers are well aware of their ISPs', other network operators', and/or enterprise email providers' security policies and procedures. It will be particularly important to relay information related to recommendations #2, #3 and #5.

Another Task Force working group, the Working Group on Public Education and Awareness, has developed a multistakeholder public information and awareness campaign to educate, most specifically, Canadian end users about what they can do to limit the amount of unwanted commercial email they receive.

8. **ISPs and other network operators should implement email validation on all their Simple Mail Transfer Protocol (SMTP) servers (inbound, outbound and relay).**

Email validation would ensure that only authenticated clients are allowed to send email via the server. For example, SMTP authentication is an enhancement to SMTP servers to enable them to verify the identity of email clients. The protocol works by requesting the user name and password of the email sender and validating this against preregistered clients. This procedure can be used to reduce spam messages, since these messages are unlikely to be from registered users in the SMTP authorization list.

9. **Non-delivery notices (NDNs) should only be sent for legitimate emails.**

Message transfer agent (MTA) administrators and spam-filter manufacturers have now generally accepted this practice. When a message is sent to a nonexistent user account, the MTA responds stating that the user does not exist. This can cause problems when a spammer spoofs a large number of addresses from a domain. Each nonexistent address generates a non-delivery response from the mail server. The MTA software should be configured not to send non-delivery messages for spoofed addresses.

Blanket cessation of NDNs may, however, create some problems for users who, for example, have mistyped an email address and are assuming that the message reached its destination.

10. **ISPs and other network operators should ensure that all domain names, Domain Name System (DNS) records and applicable Internet protocol (IP) address registration records (e.g. WHOIS, Shared WHOIS Project [SWIP] or referral WHOIS [RWHOIS]) are responsibly maintained with correct, complete and current information. This information should include points of contact for roles responsible for resolving abuse issues including, but not limited to, postal address, phone number and email address.**

Identifying the points of contact for ISPs and network operators is crucial for managing the abuse of email communication systems. All email messages include information such as DNS host names, IP addresses, and other records relating to the source, transmission, and destination of the message. The ISPs or other network operators responsible for sources of the email messages should be easily and accurately identifiable. All fully qualified domain names (e.g. hostname.domainname.ca), domain names and IP addresses should be registered and maintained with information allowing such identification.

Network operators should also ensure that domain name records; forward and reverse DNS records; and WHOIS, shared WHOIS Project (i.e. SWIP) or referral WHOIS (i.e. RWHOIS) records are responsibly maintained with correct, complete, and current information. For example, American Registry for Internet Numbers WHOIS records should include an OrgAbuseHandle including contact information for those responsible for managing abuse originating in that network. ISPs and network operators are responsible for maintaining registration information, DNS records and other identifying information in accordance with the relevant Request for Comments (RFCs) such as RFC 2142 — Mailbox Names for Common Services, Roles and Functions.

11. ISPs and other network operators should ensure that all their publicly routable and Internet-visible IP addresses have appropriate and up-to-date forward and reverse DNS records and WHOIS and SWIP entries. All local area network (LAN) operators should be compliant with Request for Comments (RFCs) 1918 — "Address Allocation for Private Internets." In particular, LANs should not use IP space globally registered to someone else, or IP space not registered to anyone, as private IP space.

Forged email-header information is common in spam and email malware. Ensuring that all publicly routable and Internet-visible IP addresses have appropriate and up-to-date forward and reverse DNS, WHOIS and SWIP registration records is very important for being able to identify the sources of email and other online communication methods. Identification of the source provides the information required to contact the responsible ISPs or other network operators, so that they can take appropriate actions to address spam or other concerns involving protocol. IP addresses registered to another organization should not be used within private networks, as their use can significantly complicate efforts to identify the ISPs and network operators responsible for an email message. DNS host names may also be used by recipients to determine access policy, but should be chosen carefully in order to avoid recipients choosing overly broad filtering policies that have the potential to block valid email. Please see Recommendation #10 regarding recommendations for maintaining correct, complete and current information.

To assist with identification of email sources, it is also suggested that email servers should have DNS host names that clearly differentiate these servers from consumer or business desktop addresses. Host names should exist and match in both forward (resolution of host name to IP address) and reverse (resolution of IP address to host name) DNS entries. ISP customers who are permitted by policy to operate email or other servers will benefit from this by having the ability to operate customized forward and

reverse DNS within their domains, thus distinguishing hosts from residential or policy-prohibited hosts. This lets email recipients establish systems that differentiate between legitimate email servers and hosts that may be sources of spam.

Residential, dynamic or policy-restricted IP addresses should also have a clear and consistent forward and reverse DNS naming convention. For example, access-control policies enacted by email recipients which differentiate between trusted and untrusted email sources are easier to establish for naming conventions that include the domain owner; service class; static or dynamic assignment; and other identifiers, such as an IP-pool identification. This can prevent ISP customers who are permitted to run email servers from being blocked due to their being indistinguishable from illegitimate email sources. Naming conventions with a "most-significant-to-the-right" scheme simplify filters and reduce the likelihood of access-control policies affecting legitimate email sources. For example, such a naming convention for the residential, dynamic IP address "1.2.3.4" at ISP Example.ca would be "4-3-2-1.dyn.res.example.ca." A sample naming convention for the small business, static IP address "1.2.3.4" at ISP Example.ca would be "4-3-2-1.static.bus.example.ca." A sample naming convention for an email server used by Smallbizcustomer.ca would be "mail.smallbizcustomer.ca."

12. ISPs and other network operators should prohibit the sending of email that contains deceptive or forged headers. Header-tracing information should be correct and compliant with relevant RFCs, including RFC 822 and RFC 2822, and reference domains and IP addresses should have up-to-date, accurate registration information.

Accurate email-header information is important for ISPs and other network operators to be able to identify sources of spam and email malware within an ISP's network. Please see Recommendation #10 regarding recommendations for maintaining correct, complete and current information.

While internal networks will often use private IP addresses (as per RFC 1918 — Address Allocation for Private Internets) that are not externally routable or identifiable, email providers should ensure that the sources of email messages are accurately identifiable for policy- and law-enforcement purposes.

Conclusion

Spam is a multifaceted, global problem that requires coordinated action on several fronts in order to achieve real and measurable progress. Implementing these recommendations can help reduce many of the worst types of spam, forgery and spoofing that occur in email. These measures will not stop spam entirely, but will significantly enhance the Internet community's ability to trace the sources of spam and hold senders accountable for their actions. The recommendations are also expected to provide the foundation on which future solutions can be built.