SECURITY

Spam Fighting Business Models— Who Wins, Who Loses

Rebecca Wetzel

Can technology defeat unwanted email? Or will the "arms race" simply continue?

In our attempts to thwart spam, will we destroy email as a reliable and legitimate means of communication? In a state of wishful thinking, anti-spam technology vendors would have us believe their solutions benefit all but spammers.

But consider this story: When three emails proposing this article to *BCR*'s editor met with uncharacteristic silence, I became concerned about his health and picked up the phone. Thankfully he was hale and hearty—but he had not received my email. A fourth attempt made during our phone call also failed—yet a test message zipped through. A filter apparently misidentified my email about spam—as spam—and blocked it. The workaround? Our trusty fax machines.

Much has been written about the technical pros and cons of alternative spam fighting approaches. Missing has been an analysis of how each alternative affects all stakeholders—senders (i.e., spammers, legitimate businesses, and individuals), ISPs, enterprises and email recipients.

TABLE 1 Vendor Technical Approaches

PRODUCT	APPROACH		
	Content-based Filtering	Sender-based Filtering	Challenge/ Response
Brightmail	✓	✓	
Clearswift MIMEsweeper	✓		
Cloudmark Authority	✓		
Cloudmark SpamNet	✓		
DigiPortal Choice Mail	✓	✓	✓
FrontBridge TrueProtect	✓	✓	
Goodmail			
interMute SpamSubtract PRO	✓	✓	
IronPort Bonded Sender Program			
IronPort SpamCop		✓	
Mailblocks			✓
Mail Frontier Gateway	✓	✓	✓
Mail Frontier Matador	✓	✓	✓
Mail Washer Pro	✓	✓	
Network Associates SpamKiller	✓	✓	
Postini Perimeter Manager	✓	✓	
Qurb		✓	✓
Spam Arrest		✓	✓
SpamAssasin (Freeware)	✓	✓	
Sunbelt Software iHateSpam	✓	✓	
SurfControl	✓		
Tumbleweed	✓	✓	
Vanquish		✓	✓

Rebecca Wetzel is an industry analyst, consultant and writer. She is president of Wetzel Consulting LLC, and is an associate with network technology and performance analysis firm NetForecast. She can be reached at rwetzel@rwetzel.com.

It's time to examine the importance of aligning the interests of legitimate stakeholders, and to identify approaches which can achieve that alignment. This article sets out to do just that.

Email Stakeholders

Soon after my colleagues at BBN unleashed the first email message, email became a mainstay of our work and personal lives. Almost as quickly, would-be marketers identified email as a nearly free means to advertise to anyone with an email address. The spammer thus became an unwelcome stakeholder in the email delivery system.

The spammer's one-to-all *modus operandi* threw a monkey wrench into the alignment of interests among legitimate email delivery system stakeholders. The enticing economics of free direct-to-consumer advertising swelled the volume of email traffic with which ISPs and enterprises must cope. It also deluged recipients with unwanted messages, sabotaging email as a legitimate means of commerce.

Spam Fighting Models

Every ISP, enterprise and email recipient craves spam relief, and scores of product vendors and service providers are peddling hard to provide relief. The most common approach is to apply technology in the form of content-based filtering, sender-based filtering, and/or challenge/response mechanisms to identify and block spam.

New to the scene are economic approaches, which add payment systems for bulk email senders to discourage spammers, while enabling legitimate email for commercial use. Predictably, state and federal legislators have also entered the fray, crafting laws to reduce spam through legal penalties.

The technological models (described in Tables 1 and 2) include:

■ **Filtering:** Filtering is available in service or product forms. ISPs provide spam-filtering services, or email can be diverted through a third party filtering service. Product-based offerings include filtering software or appliances within a network, or software on individual PCs.

Content-based filters draw on a variety of spam identification methods ranging from pattern recognition to recipient complaint systems to Bayesian filtering, a technique that uses words or character strings to identify email as spam, and learns to identify new spam the more incoming email it analyzes. Filters can generally be tuned to different sensitivity levels, with less sensitive set-

Filtering and challenge/ response are the most common anti-spam technologies

		SOLUTION LOCATION		
Sender to ISP (or Third Party) Payment	Sender to Recipient Payment	Desktop	Enterprise Edge	ISP or Central Site
			✓	✓
			✓	✓
			✓	
		✓		
		✓	✓	
				✓
✓				✓
		✓		
✓				✓
		✓		
				✓
			✓	
		✓		
		✓		
			✓	
				✓
		✓		
				✓
		✓		
		✓	✓	
			✓	
			✓	
✓	✓	✓	✓	✓

TABLE 2 Impact On Stakeholders

Solution Type And Location	Sender Type		
	Spammer	Ethical Bulk Emailer	individual
No solution	 Spam sent and all is delivered	 Reputation tarnished, commerce curtailed, all email delivered	 All email delivered
Filtering at ISP or central location	 Spam sent, some is delivered, workarounds required	 Reputation tarnished, commerce curtailed, much email blocked	 Some email blocked
Filtering at enterprise edge	 Spam sent, some is delivered, workarounds required	 Reputation tarnished, commerce curtailed, much email blocked	 Some email blocked
Filtering at desktop	 Spam sent, some is delivered, workarounds required	 Reputation tarnished, commerce curtailed, much email blocked	 Some email blocked
Challenge/Response at ISP or central location	 Spam sent, most not delivered, workarounds difficult	 Reputation tarnished, commerce curtailed, much email blocked	 Email delivered challenge/response irksome
Sender-to-third party payment at ISP or central location	 Spam sent, some not delivered, workarounds required	 Reputation enhanced, commerce partially enabled, third party (not individual recipient) determines what is delivered, email wanted by some recipients blocked by complaints from those who don't want it	 Some email blocked
Sender-to-recipient payment at ISP or central location	 Places cost on sending spam, eventually eliminates spam at the source by rendering it uneconomical	 Reputation legitimized, opens email for legitimate commerce, individual recipient (not third party) determines what is received, all wanted email is received, sender knows whether or not individual recipient wants email, allows accurate targeting of direct email	 All email delivered

Sending ISP	Receiving ISP	Enterprise	Recipient
 Spam handling costs incurred	 Spam handling costs incurred	 Spam handling costs incurred	 Spam clogs email box
 Spam handling costs incurred	 Spam handling costs incurred	 May reduce spam handling costs	 Some spam received, some legitimate email not received, third party determines what is blocked
 Spam handling costs incurred	 Spam handling costs incurred	 Spam handling costs incurred	 Some spam received, some legitimate email not received, third party determines what is blocked
 Spam handling costs incurred	 Spam handling costs incurred	 Spam handling costs incurred	 Some spam received, some legitimate email not received, third party determines what is blocked
 Spam handling costs incurred	 Somewhat reduced spam handling costs	 Somewhat reduced spam handling costs	 Some Spam received, some legitimate email not received
 Spam handling costs incurred	 Somewhat reduced spam handling costs	 Somewhat reduced spam handling costs	 Some spam received, some legitimate email not received, third party determines what is blocked
 Dramatically reduced spam handling costs	 Dramatically reduced spam handling costs, revenue received for bulk email	 Dramatically reduced spam handling costs	 Spam-free mailbox revenue received for unwanted email from ethical bulk emailers

Newer systems impose payments on bulk e-mailers

tings allowing some questionable email through, and more sensitive settings blocking questionable email, at the risk of false positives.

Sender-based filtering blocks based on a sender's reputation—with filtering decisions made using information in "black lists" or "white lists". Email from senders of ill repute is filtered, whereas email from "white-listed" senders is always allowed through. A sender can be blacklisted by such actions as sending too much email during a suspiciously short time, or by being the subject of complaints.

Many anti-spam vendors including Brightmail, Tumbleweed, DigiPortal, Frontbridge, InterMute, Mail Frontier, MailWasher, Network Associates, Postini, SpamAssassin and Sunbelt Software employ both content and sender-based filtering. Brightmail's Logistics and Operations Center uses people and technology to identify spam and its perpetrators. The center uses several million "honey-pot" email accounts, on the premise that if these dummy accounts receive email, it's safe to conclude it is spam. Information about the spam and spammers is then incorporated into constantly updated filtering rules.

Effects of Filtering: Filtering can effectively reduce spam on the network and/or at the desktop, but it can have drawbacks. The higher the spam capture rate, the greater the chance of blocking wanted email. No matter how low the risk, undelivered email can hurt business. In the case of my communication with *BCR*'s editor, neither of us knew anything was amiss. He did not know that I had submitted an article concept, and I didn't know he hadn't received it until an unusual response delay tipped me off. Businesses depend on email, and undelivered messages are bad.

At best, filtering provides perfect veto power—but this risks closing email as a medium of open exchange and commerce. One person's spam may be another's welcome email—and if third parties or groups of complainants define spam without regard to individual recipients' preferences, censorship results.

An added problem is an endless arms race between filter vendors and spammers working to trick filters into letting their messages through.

■ **Challenge/Response:** Challenge/response systems force unknown senders to prove they are human by making them solve a visual puzzle that is easy for a person but hard for a machine. The theory is that since machines, not people, usually send spam, failure to meet the challenge identifies the sender as a spammer. Challenge/response systems are often used with "white lists," so if a sender passes muster, he or she is added to a list of approved senders.

Among vendors, Mailblocks relies on challenge/response as its primary method, and several other companies, including DigiPortal, Mail Frontier, Qurb, Spam Arrest and Vanquish use challenge/response in combination with filtering.

Effects of Challenge/Response: Like filtering, challenge/response technology helps reduce spam volumes, especially when combined with filtering. But it, too, has drawbacks for some stakeholders. One drawback is that an unresolved challenge may block incoming mail from legitimate sources such as newsletters, email lists, and other email from legitimate bulk sources. To circumvent this, a legitimate bulk sender must shoulder the burden of employing a person to respond to each challenge.

Responding to challenges can also be irksome and time-consuming for individual email senders. Ironically, challenges themselves are sometimes treated as spam and removed by a filter—or even by an unsuspecting sender.

Economic Models

Spammers' interests are financial. Even if terabytes of spam are intercepted by anti-spam technologies, enough is likely to get through to keep spam profitable. This realization has spawned approaches that change the economics of spam by imposing a financial liability on bulk emailers, with the hope this will open email as a conduit for legitimate commerce and close it to illegitimate email. Two economic models are in early deployment—a sender-to-third-party payment system, and a sender-to-recipient payment system.

■ **Sender-to-third-party Payment Systems:** IronPort Systems and Goodmail Systems are implementing sender-to-third party payment systems. Goodmail requires bulk emailers to attach paid stamps to outgoing messages. These encrypted stamps include verification of the sender's identity, and they require the sender to honor an "unsubscribe" mechanism. Participating ISPs receive a portion of the stamp revenue in return for safe passage of stamped mail to recipients.

By posting a financial bond, IronPort's Bonded Sender Program allows legitimate bulk emailers to bypass filters in participating ISPs. If consumer complaints exceed one per million email messages sent, the bond is debited and the proceeds donated to non-profit Internet education organizations. IronPort's Bonded Sender Program accepts complaints from a variety of sources, including complaint departments at ISPs and IronPort's own abuse desk.

Effects of Sender-to-third-party Payment Systems: The current crop of sender-to-third-party payment systems is designed primarily to prevent legitimate bulk email from being blocked by spam filters. These systems open email as a conduit between enterprises and prospects and customers, which is normally closed by filters. Assuming bulk emailers use lists of recipients likely to welcome their email, this burnishes the reputation of email as a legitimate means for unsolicited commercial communication.

As with filtering, however, this filter-bypass system empowers third parties, not recipients, to

determine what flows into inboxes. Recipients have little say in what they receive, except to complain—which, in the case of IronPort's Bonded Sender Program, can cause the sender to be monetarily penalized and/or stop a bulk mailing.

■ **Sender-to-recipient Payment Systems:** Bill Gates has expressed Microsoft's interest in a sender-to-recipient payment system—but so far only a startup by the name of Vanquish has debuted such a system. In the Vanquish model, emailers post a bond for the privilege of delivering email to an individual's inbox. Email recipients—and only email recipients—decide whether email from an unknown bonded sender is unwanted.

Email from bonded senders contains an active icon that a recipient can click on to identify email as unwanted. Clicking this icon sets three things in motion: The recipient and the receiving ISP each receive a payment, and the sender is informed that the recipient has identified the email as unwanted. Vanquish combines this approach with challenge/response and "white list" technology to block unbonded email from unknown or unsolicited sources. With this model, unlike stamps and filter bypass systems, email remains essentially free for all except undesirable email.

Effects of Sender-to-recipient Payment Systems: A sender-to-recipient payment system has intriguing potential for aligning the interests of legitimate stakeholders in the email delivery system. It is the only approach to date that empowers an individual recipient to decide when a message is unwanted. It allows the recipient to set his or her compensation level for receiving an unwanted message. And most importantly, it relays that information back to the sender.

The result should be to reduce unwanted email at the source. Because email is reduced at the source, the result over time should be to reduce the spam burden on ISPs and enterprises.

The jury is out on whether a sender-to-recipient system will work well in practice. If it proves onerous to recipients, or if it is too complex or difficult to achieve widespread adoption, it could be a flash in the pan.

Legislative Models

In January 2004, U.S. federal legislation aimed at curtailing spam took effect. Called the "Controlling the Assault of Non-solicited Pornography and Marketing Act of 2003" or CAN-SPAM Act, this law superseded more than 30 state laws covering spam. The legislation dictates that spam be truthful, that spammers not disguise themselves with false email addresses or misleading subject lines, that pornography be labeled, that messages offer an opt-out procedure and that the FTC implement a "do not spam" list similar to the "do not call list" for telephone marketers.

Effects of Legislation on Stakeholders: The legislative approach is proving quixotic because tracking spammers is difficult, and U.S. law cannot be applied to firms outside the country, enabling spammers to operate outside U.S. jurisdiction to evade prosecution. Opt-out procedures mandated in the legislation have been used by spammers in the past to validate addresses and then sell those addresses to other spammers, making recipients reluctant to take advantage of opting out. Add to that reduced state and federal budgets, making it unlikely that enough resources will be available for legal enforcement, and the legislative solution is likely to be stillborn.

Legislative action against spam will likely prove futile

Conclusion

For years to come, technology will be king in the quest to stop spam. But no matter how sophisticated spam-fighting technologies become, they cannot solve two fundamental problems. They cannot stop spam—they can merely be weapons in an ever-escalating arms race. And they cannot fully open email to legitimate commerce.

For email to realize its potential as a means of open commercial and personal communication, the economics of email must tilt in favor of all legitimate stakeholders. In theory, the best way to achieve this is through a contract between senders and recipients—so recipients can say: "I do not want this particular email," resulting in a financial consequence that motivates the sender to behave. Legislating good behavior cannot work, although legislators will try until they are blue in the face.

I support a workable, economically based system, which when widely implemented will align the interests of all legitimate email stakeholders. Until then, we must live with nostrums that can treat the symptoms, but not cure the disease—and email will remain hobbled and compromised as a means of open communication□

Companies Mentioned In This Article

Brightmail (www.brightmail.com)
DigiPortal (www.digiportal.com)
Frontbridge (www.frontbridge.com)
Goodmail Systems (www.goodmail.com)
InterMute (www.intermute.com)
IronPort Systems (www.ironport.com)
Mail Frontier (www.mailfrontier.com)
Mailblocks (www.mailblocks.com)
MailWasher (www.mailwasher.com)
Network Associates (www.networkassociates.com)
Postini (www.postini.com)
Qurb (www.qurb.com)
Spam Arrest (www.spamarrest.com)
SpamAssassin (www.inboxcop.com)
Sunbelt Software (www.sunbeltsoftware.com)
Tumbleweed (www.tumbleweed.com)
Vanquish (http://vanquish.com)