Why Challenge/Response Makes Sense

By Dan Wallace
Vice President of Marketing and Business Development
DigiPortal Software, Inc.

There are several competing approaches to spam blocking, but only one of these works reliably. We call it "Identity-Based Challenge/Response." What this really means is treating your email inbox the same way you treat the front door of your house. For me to come in, you have to know who I am and what I want. Unless you have answers to those questions, the door stays shut. And even when you have the answers, you still may decide not to let me in. In either case, it should be your choice.

This discussion starts with a basic premise – that you have the right to manage your privacy, to admit to your personal space only those whom you know and trust. All systems aimed at helping you do so, whether involving your email, your telephone (i.e., caller ID) or your actual front door, either constitute attempts to answer the most basic privacy management questions – "Who are you? What do you want? – or are proxies for them, attempts to guess at the answers and help you make the right decision.

Our message is simple – real information is always better than guesswork. Identity-Based Challenge/Response is the only method of email management that will reliably free you from unwanted email and give you the tools to make sure you do not miss any mail you want. Properly implemented, it is both reliable and free from obsolescence. And the more people who use it, the better it works.

The "Identity-Based" portion of this methodology is simple and non-controversial. Any system that processes email based on identity is principally interested with the specific identity of the sender (not the network or server from which the sender's message was sent, which is how most current spam filters work). This method works because it is far easier to decide whether email is legitimate and wanted if you know who sent it than if you only have an approximation of this information, such as the identity of the server from which the message originated.

In the real world, the sender's email address is used as a proxy for the sender's actual identity. This has proven to be a perfectly effective proxy. Smart identity-based programs pre-approve senders by building a list of people the user presumably wants to hear from (i.e., those in the user's address book) and adding addressees on any future email. The principal is that if I send you mail, it is reasonable to assume that I am interested in getting mail from you as well. Of course, smart programs also let you change who is pre-approved. You may decide in the future that you do not want mail from me and need to have the ability to take me off your approved list.

The "Challenge/Response" part of this software model is far more controversial. The reasons for this controversy are not entirely clear, but it is clear that a portion of the technology community believes that sending out challenge messages is wrong. The objections appear to be driven in part by a belief that it is somehow wrong for senders to be asked to identify themselves, and in part by a belief that a large number of challenge messages will be bad for the Internet.

We believe these objections are simply wrong. In fact, we believe that within three to five years, it will be standard, accepted practice in all email environments for senders to expect to identify themselves before their mail is accepted by a recipient by whom they are not known. Ask yourself how many people you know whose homes you would be comfortable entering without knocking, announcing yourself and being invited in. We believe that the social norm that we all apply to our front doors today will soon be applied to our email inboxes as well.

The reason for this is simple: It works. It is relatively easy for an email program to allow into the inbox messages from email addresses that are on a whitelist. The hard part is figuring out what to do with the rest of the incoming email. The most obvious answer is to ask who the sender is and what he or she wants. The notion that it is somehow inappropriate to ask these questions is simply ludicrous. You have every right to know conclusively who sent you a message and what its purpose is before deciding whether or not to accept it.

Rather than doing this, most anti-spam programs filter mail using algorithms and heuristics which look at a combination of the content of the message and the server it came from. These filtering systems have two things in common. First, all of them represent efforts to avoid asking, and thus to guess at the answers to, the questions – "Who are you and what do you want?" Second, they do not work very well. They typically top out at about 85% accuracy – many users' experience is much worse – and are prone to both allowing spam in and discarding legitimate mail. They also degrade rapidly over time as spammers figure out how to beat them.

Effective means to query senders did not exist until recently. To understand why, it helps to remember that email is a relatively new phenomenon. Proprietary WAN-based email is only about 15 years old, and Internet-based email is only a little more than 10 years old. We have been living with email for only about half the time we have been living with cell phones. In the early days of email, the only way for someone to get your email address was for you to give it to them. This was a *de facto* permission system. The volume of email was small, and you only heard from people whom you had invited to email you by giving them your address.

As a consequence, we quickly developed habits around email use that presumed that there was no need to erect additional barriers to intrusion. We learned to treat our electronic inboxes like our physical mail boxes, where the unwritten rule is that anyone can send me anything they want, and if I don't want it I can just throw it away.

In the late 1990s, email addresses began to be bought, sold and gathered illicitly, so that your email address might be in the hands of many senders to whom you had not given it. Even then, the volume of unsolicited, unwanted email remained modest. In the last several years, however, it has exploded. Spam now accounts for well over half of all email – some estimates place it as high as 70 percent – and it continues to grow.

Clearly, our initial habits regarding email no longer make sense. The very reason that email emerged without a process to verify the identity of unknown senders – that there was in essence no such thing as an unknown sender – is gone forever. The things that arrive unbidden in an unprotected email inbox today range from the useful to the annoying to the offensive, and even the fraudulent. As we have established, you have the right to know who is sending you mail and what they want. You now have the means to do so, both effectively and efficiently.

So the question is not why you would want to require unknown senders to verify their identity but why in the world you wouldn't. Without a conscious thought, you both require this information of anyone who appears at your door and willingly provide it when you appear at the door of someone else's home. The same will soon be true of email.

The only remaining question is whether issuing the challenge messages is somehow bad for the Internet. Not only is it not bad, we believe it is the only thing that will actually make spam go away. To understand why this is so, we need to look at how an individual mailbox is treated and then extrapolate to the Internet email system as a whole.

My inbox is protected by our product, ChoiceMail One. It is 100 percent immune to spam. Mail from senders whom I have not approved is held in a quarantine folder while challenge messages are issued to the senders. For an email marketer to have any hope of reaching me, he must do three things. First, he must use a legitimate subject line so that if I happen to look in my

quarantine folder, and if he happens to be selling something I am interested in, I can tell from the subject line what that might be. Second, he must use a legitimate return address. Why? Because otherwise he will not get the challenge message. Third, if he really wants me to see his message, he needs to employ a human being to reply to the challenge because ChoiceMail's verification process requires human intervention. Any mail which does not meet these requirements gets thrown away automatically. It does not get into my inbox. I never see it.

The economics of spam are incredibly lopsided. An investment of as little as $15,000 enables a spammer to send out several million messages a day. There is virtually no variable cost associated with this activity. The spammer's game is to hope that some of those messages will make it into recipients' inboxes, and that a tiny fraction of those recipients will choose to refinance their mortgage, buy Viagra online or purchase all-natural genital enhancement. Because the spammer's costs are so low, even a tiny response rate is profitable – which is, of course, why there is spam.

But it still requires a response. As lopsided as the economics of spam are, if every inbox were protected the way mine is, even those lopsided economics would cease to make sense. When the world adopts Identity-Based Challenge/Response en masse, and it will, spam will immediately cease to exist for the simple reason that it won't make economic sense any more.

Email marketers have every right to send messages advertising anything they want (within the bounds of legality), and recipients have the right to accept and respond to such messages if they wish. But in an Identity-Based Challenge/Response world, email marketers will quickly figure out that only legitimate marketing mail (including a real subject line and a valid return address) has any hope of getting through, and then only to people who are actually interested in what is being offered. Everything else will just bounce off.

The requirement that email marketers have human beings available to respond to challenges will change their economics dramatically. This is a real cost (as distinguished from artificial costs, such as the ridiculous proposal to charge email "postage".) Is it reasonable to expect email marketers to incur such costs? Of course it is. Direct mailers incur the costs of printing and postage. Telemarketers incur the costs of staff and telephone charges. Why should email marketers be immune? You and I have every right to protect ourselves from unwanted email. If a marketer is not selling product valuable enough to enable him to afford to respond to challenge messages, he does not have a viable business proposition. Since this is almost certainly the case for the vast majority of spam solicitations, these solicitations will simply evaporate in an Identity-Based Challenge/Response world.

We at DigiPortal Software are certain that this transition will take place, although the exact timing remains unclear. Besides the email marketers, whose issues are addressed above, there are two major communities of influence and/or interest in this debate: the press and the ISPs (especially the major, integrated ones like AOL and MSN).

Some ISPs have expressed concern that large-scale adoption of challenge/response systems would flood them with additional email traffic. This view is extremely short-sighted. The major ISPs are flooded with unwanted email now, both because their subscribers are high-value spam targets and because their mail server addresses are frequently hijacked by spammers. They spend heavily on filtering systems, as well as people and infrastructure to deal with all of this unwanted mail.

The best thing the ISPs can do to improve their situation is contribute to the elimination of spam. As we have established, the most (indeed only) effective way to do this is to adopt Identity-Based Challenge/Response email management themselves. The integrated ISPs can do this by incorporating such email management into their client software. Smaller ISPs can offer it as a service. While ISPs may see an increase in email traffic in the short term, it is important to

remember three things. First, challenge-related email is absolutely legitimate, reflecting the right of users to protect themselves, and therefore something they are obligated to carry. Second, large scale adoption of Identity-Based Challenge/Response will quickly drive both the volume of spam and the the related volume of challenge messages down. Third, as soon as they adopt this approach to email management, the ISPs can drop their largely ineffective filtering systems and stop investing time, energy and money in unproductive efforts to deal with spam. Email will be either accepted or blocked by users, and when blocked can simply be throw away. (It should be noted that this last benefit applies to corporations and other organizations as well.)

This brings us to the technology press, particularly that portion of the press which reviews products, expresses opinions and influences the direction of the market. The dramatic increase in the amount of spam is no secret. Neither is the overwhelming superiority of Identity-Based Challenge/Response systems over any other approach, real or proposed, to spam elimination. What often goes unmentioned is the fact that, as described above, this method of email management will work best when it is the norm. Simply put, an Identity-Based Challenge Response world is a world without spam, period.

Therefore, we believe this sector of the press has not just an opportunity but a duty to encourage the market to adopt Identity-Based Challenge/Response email management. The large-scale adoption of this anti-spam methodology is a virtual certainty for the simple reason that it works, and is the only solution, whether actual or proposed, that works. The timing of the adoption of this technology remains uncertain, but the sooner it happens, the better for all of us. In accelerating this transition, the press can and should play a valuable role.