It could have happened on any sequence of days, but it all happened on one day. Earlier this month, at the Online Publishers Association Summit in Palm Beach, some innocent asked about e-mail marketing. “Too much of a taint from spam and phishing,” the panelists agreed.

Later that same day, we wanted to reserve a trip on the Albuquerque-Santa Fe shuttle. But the URL for SantaFeShuttle.com quietly redirects to SandiaShuttle.com, which is actually another company - and not the one we wanted. The difference is not clear when you’re on the Web, but it’s amply clear when you’re at the airport, where the two services sit side by side across from baggage claim 3. They are engaged in a lawsuit over the domain name.

And finally, on the flight to Albuquerque, we watched a “60 Minutes” episode – heart-rending tales of families torn asunder: a mother who wanted to know if her son was okay, but couldn’t bear to talk to him because he had stolen from her; a sister estranged from another sister who had charged $50,000 under the first sister’s identity. Indeed, it was the same old tales we’ve had since antiquity, rendered newsworthy by that most modern of maladies, identity theft.

The Net is losing its appeal to many because of the proliferation of spam and phishing schemes, so-called joe jobs where innocent users get bounce messages meant for someone else, compromised machines used to send out spam or viruses, spoofed e-mails and websites, identity theft and all manner of trash and threats.

It’s ironic, because the Net should be a safer place than the physical world. You don’t need to engage with people you don’t want to,
and things in theory are more trackable. It is easier to keep strangers out – if you wish to.

But it is also harder to figure out who people are. That has led – in our trusting world – to a very open Net in which strangers roam. But if you change the default – from everyone’s a stranger to no strangers allowed – you can create a very different world. We’re about to change that default. Instead of starting open, systems will start closed. Everyone will deal only with identified, trusted, accountable counterparts, in the peer-to-peer accountable Net.

The premise of the accountable Net is that we don’t need government regulation to help us reopen the closed, safe world into a broader yet still rule-based public space. Geographically constrained governments are ill-equipped to maintain security across the global Net other than in extreme cases; virtually local, private action works better. The accountable Net takes into account individual preferences, and it makes parties accountable to one another rather than to government rules that may not suit everyone. Users can choose which regime they want to "live" in: People who want more regulation can choose to interact with parties governed by such regimes, while people who want to lie and cheat will find themselves in the company of others similarly inclined. You can tell which is which by reputation systems, brands and ultimately, perhaps, by domain names or the "certified mailer" programs described later in this issue. (Government can still play a helpful role, both in pushing the private sector to regulate itself if only for fear of regulation, and in punishing criminals/forcing redress where market forces and self-selection cannot do the job.)

Like so many other things, governance works better when it is peer-to-peer or occasionally clustered (but not centralized). With adequate information about their counterparts, reliable reputation systems (see Release 1.0, October 2003) and protective tools and services, users are best-equipped to make decisions for themselves, or to delegate those decisions to specific parties whose approach they trust and who are in turn accountable (through the rules of competition) to their customers. They’re also best-equipped to affirmatively create networks of communication relationships. The
accountable Net is not just about keeping people out; it’s also about people joining together.

For this P2P paradise of governance to work, however, we need two things:

• reliable ways of authenticating people and organizations on the Net so that reputations and the rules that entities live by can be firmly attached (only) to the entities that have earned them, along with tools and services that individuals and organizations can use to see and interpret this reputational information. Only if you have that underlying infrastructure of authentication of identity can you build reliable reputation and accountability systems. That doesn’t mean that anonymity should be impossible – but that anonymity should be apparent, and that individuals can then decide whether and how to engage with anonymous parties. (Note: You can also be anonymous and benefit from credentials – i.e., have some other person or organization who does know you vouch for your behavior, either overall or in certain contexts such as sending a message, engaging in a transaction or making an online posting.)

• a web of accountability, extending and expressing the power of individuals to make their own choices through software, organizations and services that can work collectively to reflect users’ opinions, to aggregate their market power and to disseminate reputations and enforce accountability. This means everything from software vendors’ tools, to reputation services, communities with their own rules and services that monitor their members’ behavior in exchange for certain privileges. They act on behalf of individuals who choose to use them, rather than collectively on behalf of all people in a particular geography. However, in extremis, these organizations can help individuals claim recourse from malefactors or engage with the government to prosecute cases of fraud and other crimes.

This issue of Release 1.0 outlines some significant recent developments towards realizing the promise of the accountable Net. But it’s a vision of decentralization, and there are lots of parties and pieces that need to work together. We look at only a few of them here - primarily at the accountability of organizations from the point of view of individuals. Thus, we focus on services that help individuals identify the parties they are dealing with while protecting their own identities, rather than biometrics (for example) that let corporations identify their employees or customers (although there’s some overlap, of course). Those issues have been amply covered
elsewhere (see Release 1.0, June and July 2002). In the future, we hope to see more accountability within the domain name system and the ISPs who provide mail accounts and host Web servers.

So far, most attention has focused on keeping information secure from bad people and keeping bad people out in the first place (however you define “bad”). The problem is that you often have to give out information (say, a credit card number) to strangers in order to use it (although one can publish a credit score, for example, without revealing the information that led to the score). And how do you know who is “bad”? Hint: Authentication systems let you know who people are (or, as described in this issue of Release 1.0, who authorized them to send e-mail); reputation and accreditation systems let you know what they are – good, bad, authorized or otherwise credentialed, according to a variety of criteria.

But there’s another approach newly possible: protecting oneself in real time. You can’t keep all information secure, but you may be able to prevent its malicious use if there’s a way of protecting its owner at the time of actual danger, such as during an encounter with a spoofed website.

Specifically, we first cover authentication systems for e-mail, a key and fast-moving area. We also outline current reputation systems for e-mail, and how that market is evolving. Then we look at some of the problems and solutions for website spoofing.

Authentication Standards and E-mail

Weapons of mail destruction
The situation with spam has now gotten so bad that erstwhile competitors are banding together. The E-mail Authentication Summit the Federal Trade Commission convened earlier this month in Washington, DC, was almost a love-fest, though it didn’t result in the ratification of a single standard – Sender ID – that many had hoped for. In fact, that would not have been a desirable outcome. Spam is a great example of asymmetric warfare – and any single solution would merely concentrate the attacks. Instead, it needs something closer to an immune system, which continually evolves new antibodies to fight new threats.

The Summit did however implicitly acknowledge that the government would defer to the private sector if the private sector rose to the challenge. “Going in, there was
some concern that if we can’t come up with a solution, the government will impose one. But they seem to understand that people are working and that hurrying things would be a bad idea,” says John Levine, who participated as chairman of the Anti-Spam Research Group, an Internet Research Task Force working group. In short, the system is working with no need for “intelligent design” from above.

At the Summit, there were both proposals competing to perform almost identical functions, and a spectrum of functions ranging from identifying the server that sends mail, to authenticating servers, to authenticating individual messages. Other companies talked about their mail filters or their reputation systems.

The authentication schemes are where the action is. In a sense, they are an attempt to unify the identifiers so that reputation systems can work – and so that fake identifiers can be invalidated. In theory, an IP address belongs to a server owned by someone identified by a domain name; in practice, IP addresses come and go rapidly, and domain names are easily spoofed. Imagine a stock market where new securities were constantly being issued by entities that might or might not be associated with the companies’ names they traded under. It would be pretty tough to establish reliable pricing. That’s pretty much the situation in the mail world right now.

**Authentication as a first step**

The challenge is that the mail system began as a communication medium for trusted parties to share messages, and it is still used as such by many individuals and companies. However, it is also being used as a mass commercial medium by large-scale mailers, legitimate and otherwise. The system built for individuals is ill-suited to accommodate these two different kinds of traffic, yet it’s hard to distinguish them reliably on the scale required.

The first step is authentication, which merely helps a mail receiver (usually an ISP or a corporate filter rather than an individual) get past the spoofing so that they can then determine what to do with a piece of mail. Spoofing, when a message uses a fake sender address from a domain that is not in fact responsible for sending it, usually adds to a score rather than forces a decision: A spoofed mail may be a false positive – a forwarded mail, for example, or one sent from a mail service with a misconfigured mail system (though those numbers should diminish as standards spread). An unspoofed mail, on the other hand, may come from a spammer with a legitimate domain name but an illegitimate business – or at the best, a harmless but unwelcome
communication. Spammers can be authentic too; they’re just authentic spammers. So authentication is only part of the game, as we’ll see in the second half of this issue.

Mail services are already looking at IP addresses and domain names; checking the match between addresses and domain names is merely useful but still incremental information. There are already a number of industry-wide reputation databases in widespread use, including open-source ones such as the Realtime Blackhole List (RBL), and commercial efforts such as IronPort’s Senderbase and Habeas’s Habeas User List (available free as marketing initiatives) and proprietary ones used by vendors such as CipherTrust and Brightmail (now part of Symantec).

And finally, there are several schemes for establishing a sender’s good name (by domain or IP address) and putting it on a whitelist, including those of IronPort (page 17) and Goodmail Systems (page 22). However, any inbound mail receiver is loath to accept any other organization’s whitelist as a final decision factor; most of them use a variety of inputs to process their mail (although Goodmail is trying to get guaranteed rather than preferred delivery for its customers). As quickly as spammers change their IP addresses to avoid detection, often shifting among thousands of compromised consumer computers on cable modems, so do inbound mail services need to update their whitelists to avoid vulnerability. Likewise, organizations change their identities – and their behavior.

**Domain authentication: Two approaches**

There are two main approaches to assisting domain authentication: path-based and signature-based. The path-based approach looks at the path a message took – basically the IP address it came from – and compares it to a list of permitted IP addresses (or Sender Permitted From addresses) listed in the purported domain’s DNS (domain name system) records. Technically, the IP address is hard to spoof, since the receiving machine (or Message Transfer Agent, MTA) is in direct communication (via its IP address) with the sending MTA already. What’s easily spoofable is the domain name (or owner) the message claims to come from: It may not match the IP address. What’s coming is widespread publishing of SPF records by senders, complemented by widespread checking of those SPF records by recipients.

Of course, this method works poorly when mail is forwarded or passes through a chain of MTAs. There are ways to fix the problem, but they require extra work on the part of senders, and require each node in a chain to rely on the previous nodes’ trustworthiness. A message could be changed or spoofed along the way, or an unreli-
able forwarder could transmit sender information that it knows to be untrue or has not bothered to check. Over time, forwarders, mailing lists and other relay services will probably adapt, but for now they’re a part of the ecosystem that will have the most trouble with path-based authentication. (Note that this problem does not apply to regular e-mail service providers (ESPs) or ISPs who send out mail on their customers’ behalf, as long as those customers take care to publish the ESPs’ or ISPs’ IP addresses as authorized senders for their mail.)

The signature-based method looks at the mail itself and checks for a signature that certifies its domain of origin, which avoids the forwarding problems but imposes more overhead on both senders and recipients. Here the keys used to sign the messages can be authenticated at the sending domain.
Note that both these methods work without continuing human intervention. It’s mostly the mail servers that do the work (once they are programmed by humans). Outgoing MTAs create the envelopes or headers or sign the messages; receiving MTAs or MUAs (Mail User Agents) parse the headers and check IP addresses or verify signatures by checking back with the source.

Over time, some authentication information may be passed on to individual human recipients (with special icons for “special” mail, as with Goodmail) who can use it to make their own judgments about their mail (though that capability isn’t implemented in most commercial e-mail clients yet). Thus, a user could see either that a message was especially trusted, or by contrast, that a message from a familiar name had failed sender authentication: Does this mean that Alice is wandering through India sending from an Internet café, or that someone compromised her machine to send out viruses? Juan probably can make that judgment better than his mail server can. But he may have a harder time judging whether a message purportedly from his broker is bogus, and the authentication information will be key in his decision.

Path-Based Authentication: Where You Came From

Path-based authentication is the most lightweight authentication approach in terms of implementation burden, and of course also the most lightweight in robustness.

Sender ID Framework

The big merged standard in path-based authentication is Sender ID (or SIDF, for Sender ID Framework), the combination of two standards – Caller ID for Mail proposed by Microsoft, and Sender Permitted From, originally developed by Meng Weng Wong, founder and CTO of Pobox (most famous customer: lessig@pobox.com), and endorsed by AOL among others. (For complex political reasons not worth explaining, SPF has now been neatly renamed Sender Policy Framework.)

The basic idea is that the sending domain adds a few records to its DNS entry listing the IP addresses of its outgoing mail servers, including those of its ISPs or ESPs. Then a receiver can check the validity of mail claiming to come from, say, “release1-0.com” by checking to make sure that the IP address from the sending server matches one listed for the release1-0 domain. Of course, most inbound mail services will
cache the IP addresses of frequent senders, so that recipients won’t be pinging DNS records all the time.

But...things aren’t totally unified. As a merged standard, the Sender ID Framework has two ways to authenticate the sending domain of a message: Microsoft’s original Caller ID for Mail checks the Purported Responsible Address, which is what the user typically sees in the “From:” field. (However, if the “From:” line says “Citicorp Security” sleazyfish@citicrop.com, how many users will notice the artful typo in the actual address?) Under the original SPF proposal, the receiving MTA can check the “Mail_From” address, which is the address that receives bounce messages. Technically, the Mail_From address is in the outer message envelope, whereas the PRA is a header inside the envelope and requires an extra processing step to be read.

Private-sector politics
To check the PRA, a receiving mail server needs a license from Microsoft. (By contrast, SPF and the signature-based methods of authentication have more liberal, open-source licenses.) “It’s free and we will never ever charge for it. In perpetuity,” asserts Ryan Hamlin, GM for Microsoft’s Safety Technology & Strategy group and leader of Microsoft’s Sender ID efforts. “We’ve invested some IP in this and so has the industry. We wanted to protect not just Microsoft but the industry as a whole. Now imagine that a small company came up and tried to patent it. We want to protect the industry and Microsoft from any claims. All we ask is to take the license and understand what’s in it and that it’s royalty-free.” Take it or leave it; that’s Microsoft’s story and it is sticking to it.
That may sound one-sided, but consider the alternative. Hamlin continues: “Doing what we’re doing is a bit of a harder line [than assigning it to a standards body] but we believe it’s the right thing to do. It sounds easier but we feel we’d just be back in the same situation, funding a defense but not being in control of it.” He adds: “We all have to balance our competitive needs. But Bill Gates made it clear to me that our goal wasn’t to make more money off spam. It was to solve the problem. I could make some trade-offs here [such as keeping the license royalty-free in perpetuity] that other people at Microsoft couldn’t make.”

In short, Microsoft is going full speed ahead, and the Sender ID Framework is gathering adherents (see box, page 7). Using it as a sender is easy, says Hamlin: “It takes all of five minutes for a mail administrator. There’s a free tool on our site. All you have to do is copy the information it generates [about where you send mail from] into your DNS records.” (The challenge is more on the recipient side – figuring out what to do with the spoofed mail, and making judgments based on the reputations of the domains of the unspoofed mail. More on that later.)

Microsoft’s outgoing mail servers (including its own user base and its 30 million-odd Hotmail users) already publish full SPF records, and by the end of December it plans to check IP addresses against SPF records for all incoming mail. That’s 3 to 4 billion messages a day, says Hamlin. Go Daddy and CipherTrust, two mail services, are already checking for SPF records as part of broader mail hygiene services.

“The Sender ID train has left the station,” says Hamlin cheerfully. “There are already 200,000 domains with SPF published, and AOL, Hotmail, and Earthlink all will be checking inbound SPF records by the end of the year. We have momentum here which is great. Let’s still work on crypto [signatures], but there are costs.” He notes that Microsoft has opted to work with Cisco and Yahoo! (however they evolve jointly) rather than show up with a third solution: “I felt the pressure to merge [Caller ID] with SPF and we did. We cannot afford to have all these different crypto [signature-based] solutions.”

Caveats

Of course, there are complications with path-based checking for users sending through mailing lists, roaming users on cell phones or third-party WiFi services and hotel MTAs and the like. Most of the common use cases can be easily handled, including also those of established mail services, list managers, and remailers and forwarding services such as pobox.com or alumni and other lifelong address ser-
VICES. Generally, mail may hop around the sender’s network for a while; then it’s transferred to the recipient’s network, bounces around there, and is finally delivered. In theory, the only transfer that matters for authentication purposes is the one from the sender’s network to the recipient’s – as long as each side can trust its own team.

Certainly there will be exceptions, misconfigured mail and DNS servers and the like, but the idea is not airtight protection. Rather, it’s an incremental aid to detecting spam. Messages that “pass” can be judged by the reputation of the domain that sent them, as well as by the reputation of a “known” IP address. Messages that “fail” can be judged by other criteria, usually specific to the recipient and based on content, since the actual sender is unknown. (For example, a receiver may decide to be especially forgiving or unforgiving for mail purporting to be from domains in a particular country, from a particular known individual or with attachments of any kind.) “Not every single scenario has been put through these proposals,” says Hamlin. “It won’t accurately classify every single piece of mail. There’s a lot of discussion around fringe cases, all the ways it could fail to work. Just because you pass the SPF check, you don’t get a straight line into the inbox,” says Microsoft’s Hamlin.

What will be the impact? At first, it probably won’t be that noticeable to users. Hamlin notes that 80 percent of the inbound mail to Hotmail is from spoofed domains – much of which is already rejected. Moreover, Levine adds, “Vast numbers of published SPF records are wrong; domain registrar Go Daddy said at the FTC forum that they are telling several domain owners per day about wrong SPF records they’ve noticed on customer or incoming mail.” Not all of it is necessarily spam, but all of it is definitely worth a second look. Nor is non-spoofed mail definitely good.

“Spammers can publish their SPF records just like anybody else,” says Hamlin. “When we surveyed the early adopters, we found that about half the people publishing their SPF records are spammers. But it gives us more evidence to go after them. With your [true] domain name, I can go to the [domain name] registrar and get your credit card [with reasonable legal process]. We’re using the SPF records as one more piece of evidence.” He estimates that about 10 percent of the recent lawsuits Microsoft has filed against spammers used SPF records to tie the spammers to their mail.
Signature-Based Authentication: Who Vouches For You

Path-based authentication is only one mechanism for fighting spam. Indeed, once it gets established, the reliability of Sender ID is likely to deteriorate rather than improve: Over time, spammers motivated by greed and selected according to Darwinian principles will no doubt figure out ways around Sender ID, and the esoteric use cases will become commonplace. Most promoters of the standard figure that it’s just a step on the way to signature-based authentication, using encryption techniques to “sign” or “stamp” the mail. That requires considerably more effort, but will provide more reliable authentication. The signature ensures that the message cannot be tampered with in transit – a bogus URL in the text substituted for a good one, for example, or a header record modified. (However, the message itself is not encrypted; it can still be intercepted and read by any server it passes through – at least technically, though not necessarily legally.)

There are two primary proposed standards for signature-based authentication: DomainKeys from Yahoo! and Internet Identified Mail (IIM) from Cisco. These would-be standards are very similar, both Yahoo! and Cisco agree.

The curve of adoption for signature-based authentication is likely to be flatter than for path-based, since it takes more work per mailing authority as well as per message received than just publishing SPF records. For each corporate mail server to develop such an infrastructure will take substantial effort and expense, though certainly MTA software vendors will do everything they can to make the process easier – for a price. Yahoo!’s VP of communication products Brad Garlinghouse, for one, thinks it’s time to get started. He says: “If we as an industry know today that a signature-based authentication method is a better implementation, and it’s available today, why are we taking the incomplete step to Sender ID when we will then need all the mail administrators to add or reconfigure to support a signature-based authentication mechanism in the near future? Moreover, the overhead we are talking about is something like 10 percent. For well over 90 percent of all mail infrastructures, no incremental equipment will be necessary.”

Cisco’s Identified Internet Mail

The idea, of course, is not new, but until recently it did not seem worth the effort to sign every piece of mail. Cisco, for one, considers itself ideally positioned to develop a standard because it is a provider rather than a user of basic technical infrastructure. Says Dave Rossetti, VP of strategic software technology, “We’re on the inside of
the mail system as opposed to the outside. All the other people are outside [operating mail servers or user clients]. We had an opportunity to say, ‘What if we made the Internet stronger?’ Rather than mop up the mess after the act, how about if we got to a situation where everyone’s mail was signed with a private key?”

The issue, he notes, was to do it scalably. In short, the sending server/domain owner uses a private key to sign its mail. The Cisco approach suggests that the domain owners put up a lightweight service “near” the mail server – i.e. under their technical control - and operate their own key registration service [KRS], though they could also use the DNS (as is the default in the Yahoo! proposal). When the receiving server gets a signed mail from Cisco (or anyone else), it checks back with the KRS or the DNS to verify that the key used was authorized for that sender by that domain (and key) owner.

“At Cisco,” Rossetti continues, “the idea is to have one private key for signing all mail leaving Cisco. We vouch for all our users. At IBM, they can check and say, ‘Okay, it’s from Cisco.’ What about Yahoo!, Gmail, MSN, Hotmail? These folks are going to have to sort out what they do with their customers. We have challenged them with that.”

**Yahoo!’s DomainKeys**

In fact, Yahoo! and other mail services are quite familiar with the challenges of vouching for their users! And Yahoo!’s DomainKey system, under an open-source license, already has a number of active implementations, notably at SBC, Rogers, British Telecom, Earthlink, Google’s Gmail and of course (in rollout) its own user base – a nicely building critical mass.

“Our relationship is constructive,” Yahoo!’s Garlinghouse says of himself and Cisco’s Rossetti. “We’re both just trying to be catalysts for progress. There’s no doubt that Cisco’s and Yahoo!’s crypto solutions are close and it makes sense for us to collaborate and get closer together. I expect we’ll resolve the remaining differences by getting real-world test data and seeing what the industry prefers.”

In fact, DomainKeys works almost exactly like IIM. One difference is that DomainKeys are stored in the DNS records by default (like SPF records), leveraging the DNS as the key hosting infrastructure. Second, while IIM sends the key with the message, and requires a check back only to verify that the key is authorized, DomainKeys requires the recipient to check back with the sender’s domain to get the
key that can verify the signature. (Yes, if these sound like minor details compared to the overall concept, they are!)

The real-world testing should happen fairly quickly, given that Cisco is already signing some of its outbound e-mail with IIM and that DomainKeys already boasts widespread (for an unratified standard) adoption.

Any company that wants to can start advising its customers (directly or via DNS or KRS postings) to accept no mail from that company unless it is signed. Yahoo! and other ISPs and corporate mail recipients may develop not only whitelists, but also checklists of brands and trusted domains that sign all their mail. Banks and other financial institutions are likely to be among the first to adopt such policies, and ISPs or mail services that want to protect their customers will heed them. Any mail purportedly from these sources that is not signed (even with Sender ID authentication) would be automatically rejected.

Yahoo! itself, with 40 million e-mail accounts, is now rolling out signing and verifying to all of its user base by the end of November. “What would it take to sign all our outgoing mail?” Garlinghouse asked rhetorically as he embarked on that roll-out.

“We run a massive e-mail infrastructure. We want to test it, double-test it, run it in the real world and make sure it won’t interfere with our operations.”
“Now, if someone goes on a phishing attack [using Yahoo!’s name], we’ll either know it didn’t come from Yahoo! – or we’ll be able to close that user’s account. It’s one more push to get that first domino - the identity of the domain - to fall over.”

He continues, “We have a number of policies in place to prevent bad behavior. For example, if you’ve only been our customer for 24 hours, you have less flexibility in using mail. But we don’t go into detail. The more visibility we provide to spammers, the more they know about how to get around us.”

**User education and client-side visibility**

Unfortunately, spammers are taking the trouble to get educated about all these systems, while most users are not. As Garlinghouse notes, “One of the beauties of [DomainKeys] is that if you’re a Yahoo! mail user, you get the benefits of it without knowing or doing anything. On the other hand, over time, we want the visibility” because no one can protect users who don’t take some care for themselves.

Indeed, it would be a true disaster for users to think that Sender ID Framework or even IIM/DomainKeys makes them safe.

First of all, it will be a long time before all mail is signed. And even that won’t protect everyone. Mail from Citicrop may be properly signed by the Citicrop key service, for example. . .but it could still deceive an unwary consumer.

The user education challenge will be great. Ultimately, client mail tools and browsers will include user-friendly interpretations of various authentication metrics and reputation systems to protect users, but it will take a while for these to emerge – and meanwhile, spoofers will try to compromise those as well. (See pages 26 to 27.)

**Reputation and Recourse**

Authentication of a sender is key to any kind of reputation system, because the reputation needs to attach to some verifiable identity. In the emerging standards for e-mail sender authentication, the identity and authentication are at the domain level; each service, whether it’s an ISP, a corporate mail service or a hosted mail service, is presumed to monitor the mail behavior of its individual users. (If it doesn’t, it will get a bad reputation for itself – and may face blacklisting for all its senders, not just the offending ones.) The mail service can also respond to (or refer) complaints about the content of mail, including fraud, but the main issue here is sending behavior.
However, mailing activity – and reputations – are more granular than domains. In the world of e-mail, many IP addresses (often many of them linked to a single domain) already have reputations, while other IP addresses come and go overnight. Many of those “belong” to individual PCs on cable networks that may have been compromised by spammers; others are “regular” servers newly set up, some by legitimate little guys, and some by illegitimate bad guys. It can be really tough to tell the difference, in streams of mail pouring in from sources all over the world.

Back to the established domains: A given domain will have a variety of mail streams – personally written mails from employees, bills and other statements from accounts receivable, marketing messages of various kinds – everything from individually developed credit offers to mass campaigns for everyone who lives in northern Illinois. Says CEO Des Cahill of Habeas Inc., a mail hygiene company (Page 19): “You might not want to get yet another offer for a GM credit card, and if lots of others feel that way [and complain], that’s a big negative vote on GM.com mailstreams. So does that mean that my ISP is going to drop e-mail from GM.com and I’m not going to get my recall notification on my Chevy Suburban? At Habeas we’re doing both authentication and accreditation at the IP level - so that we can distinguish E-Loan’s marketing e-mails, from customer support e-mails, from their loan-document e-mails. These types of mailstreams all have different reputations and receive different treatment in ISP filtering.”

Thus the world of mail is in constant turmoil, even as established mailers and established intermediaries attempt to stake out safe ground. The safer the ground gets, of course, the more tempting it is to attack: Just think of all those paper mails that attempt to look like official government mailings. The same happens on the Net. That’s why inbound mail services are loath to give any kind of incoming mail or whitelist an automatic green light. Just as illegitimate senders move around to stay safe, so do receivers refuse to open up totally to any incoming mailstream, also in order to stay safe.

Below, we describe a number of mail “hygiene” vendors who are trying to keep the playing field well-lighted and level. IronPort was a company presenter at PC Forum 2002; Scott Kurnit represented Goodmail on a panel at PC Forum 2004. CipherTrust is a ready source of useful statistics for the public, as well as mail services to customers. And Habeas is a company that has changed its business model in co-evolution with the market. All of them charge senders for, in effect, warranting their good reputations and providing them a speedy path through receiving mail systems. One might say that authentication and reputation systems will render their services
unnecessary, but we think that instead they will become part of a continuum of services that help companies, especially the small guys, make their way in a fragmented world where reputation is hard to establish, and where services such as IronPort’s and Goodmail’s are easy to buy at costs well below the expected returns for the mail they accredit. It’s an irony that the largest, best-known, best-behaved companies aren’t that interested in such services, which tend to level the playing field. They already earned their good reputations the hard way, and they don’t need third parties to represent them.

IronPort Systems: Making manners matter
When IronPort debuted at PC Forum in 2002, it was an appliance company that offered a robust outgoing mail server and was trying to establish a reputation for itself and its customers. (See Release 1.0, March 2002.) Founded and run by a team of second-generation mail experts, it is now a large, successful but still private vendor of mail systems, both inbound and outbound, with a variety of value-added services (including spam filtering from Brightmail, virus detection from Sophos and encryption from PGP, among others). Most of the value-added involves filtering inbound mail, but IronPort’s mail servers can also conduct content and policy checks to make sure mail-users aren’t sending out sensitive materials or (inadvertently) viruses. IronPort now has over 1000 clients, including six of the top 10 ISPs.

Almost as a byproduct, IronPort now offers two reputation-based services, one for customers, and one for the public. The first is for so-called Bonded Senders, who want certification of a good reputation and enhanced deliverability of their mail to large inbound services such as Hotmail that support the Bonded Sender program as recipients (as a service to their own users, in essence).

Under the terms of the service, which is certified and monitored for compliance by TRUSTe (which collects a majority of the certification revenue), e-mail senders put up bonds that vary in amount depending on company size and volume of mail sent, in exchange for better mail deliverability. The pricing ranges from nominal for nonprofits to $500 for small companies and $5000 to $10,000 for larger ones. (The largest, such as, say, American Express or Amazon, don’t need such a service because they can get onto the large mail services’ whitelists directly.)
“We don’t give you your reputation,” notes IronPort CEO and co-founder Scott Weiss, formerly a top business executive at Hotmail. “You earn it through good sending practices, which are monitored by TRUSTe.” Only companies that pass an initial TRUSTe and IronPort screening of their mailing policies and practices are even accepted into the program. If a company misbehaves, its account is further debited, but the money for IronPort isn’t in the bad-behavior debits; too much bad behavior makes you a former customer rather than a profitable one. IronPort currently has more than 100 Bonded Senders, including CNET Networks, Google, QVC and Motley Fool. And, testifying to the seriousness of its claims, more than 10 senders have been booted from the program, Weiss says, even after passing the screening and paying their money. “Basically, if your bond is ever debited [because of too many recipient complaints, typically], you’re immediately put on a watch list for termination. Companies that join and start testing the perimeter with their sending practices face immediate expulsion,” he adds.

About 28,000 receiving domains, including MSN, Hotmail, Roadrunner and some other big unnamed services as well as many universities and enterprises, give priority delivery to IronPort’s Bonded Senders. Overall, says Weiss, they account for 30 percent of the world’s inboxes. The way it works is similar to how the Sender ID Framework works – except that permitted-sender records are hosted by IronPort rather than in each sending domain’s DNS records. The Bonded-Sender recipients look at the IP of the sending machine, and compare it to the Bonded-Sender list of vouched-for sending IP addresses. By limiting its customers to using designated mail servers rather than forwarders for sending their mail, IronPort avoids the complexities that can bedevil the Sender ID Framework. And, notes Weiss, “We do better [than just authentication of identity]; we accredit the behavior of domains and the sending organizations. We have a case study we did with CNET Networks that shows a deliverability uptick of more than 15 percent for Bonded Sender vs. sending without.”

**Senderbase: A rating service for mailers**

One way IronPort checks on prospective clients for the Bonded Sender program is to look into its own database of mailer behavior, which it calls Senderbase. “Senderbase is the equivalent of Equifax for all senders of mail. E-mail admins use it to look at IPs they don’t know,” says Weiss. IronPort collects mail-sender information from all its customers and puts it into Senderbase; it then uses that information across its customer base in helping them to filter spam. It assesses mailer behavior by IP address on more than 50 criteria, says Weiss, including volume and volume trends, whether a sending IP address also accepts mail (most spammers don’t because they would be flooded with bounces and complaints and retaliatory attacks), how long an IP
address has been in operation as a mail server, whether the IP address matches the sender’s purported domain name, and so forth. It also uses data from SpamCop, another IronPort property, which collects and forwards e-mail complaints from consumers and companies, as well as complaints (about senders) collected by IronPort customers such as Hotmail from their users. IronPort publishes some of the Senderbase information publicly as single-dimension scores for each IP address; the details used to calculate each score are proprietary.

Most large-volume mail receivers use data from Senderbase, Weiss believes, and it covers most high-volume sending IP addresses on the planet. “It’s a great marketing tool for us,” he says. “The people who use it are mostly mail administrators, and that’s exactly who we sell to. It’s like a coffee mug with an IronPort label – the gift that keeps on giving. You can see the rating, but if you want details you have to pay.”

**Habeas: Mirroring the market**

The story of Habeas Inc. (why didn’t they call it Habeas Corp?) illustrates how the market has changed over time, from a world of sysadmins and genuinely trusted senders, to one of consumer services and trademarked “trusted-sender” programs. It was founded back in 2002 by Anne Mitchell, a lawyer who previously worked at the Mail Abuse Protection System (or MAPS, another reputation service, and current home of the original Paul Vixie Realtime Blackhole List), and Dan Kohn, the current chairman of Habeas and a general partner at investor Skymoon Ventures.

The business model was to certify “good” senders, for a fee, and to authenticate them by allowing them to publish a copyrighted Habeas haiku in their headers. When spammers used that same haiku to try to get through filters, Habeas sued them. “We sued about three spammers successfully, but it wasn’t a scalable business model,” drily notes CEO Des Cahill, an Apple veteran who joined the company as CEO in August 2003.

Since then, he has shifted the company from running what amounted to a whitelist and delivery service, to accrediting customers and helping them better deserve to be on a whitelist. He adds: “We used to say, ‘Deliver the mail,’ and we charged $25,000 per year for that. Now we emphasize accrediting our customers and improving sender practices.”

In fact, the market for whitelists and reputation services is becoming commoditized (like stock prices), and the value-added is in more
specific information, especially for the senders. Habeas itself offers its basic reputation service, called the Habeas User List, for free to mail receivers. But to add value, it will shortly start publishing additional and more specific information about the practices of its accredited, fee-paying senders. For example, it will list seven levels of subscription permission for mailstreams in its “Sender Warranted E-mail” service, which will most likely remain priced around $25,000 per customer.

Even as all this information is increasingly available, says Cahill, many senders still don’t have a clear understanding of their own reputations – or of how to improve them. So Habeas’s emerging revenue source is constructive feedback: information products for tracking their e-mail delivery rates, specific consumer feedback and complaint-handling, ISP and blacklist reputation data for specific mailstreams, and the like. Habeas also offers senders specific advice on their practices.

“We give customers a head-to-toe check-up,” says Cahill. “We tell you how spam filters are tuned to accept and treat mail from your domains. We run you through a 42-point process. We examine and classify each of your mailstreams [i.e. the parameters in CRM database that generate different messages, depending on previous opt-ins, opt-outs, data sources and the like]. We give you feedback, and then we turn around and say to receivers, we have certified the following statements. . . .”

Cahill previously worked at Apple, Autonomy, Netscape and BridgeSpan. Ironically, in some sense he took the place of Richard Gingras, CEO of Goodmail (page 22):

When Apple closed down its own online service, eWorld, which was run by Gingras, Cahill was working for Apple and strengthened Apple’s relationship with AOL and expanded Apple.com.

Cahill’s view of his market is of an exchange with inadequate data, a pool of participants with few feedback loops. “This market of volume senders and receivers (ISPs) is insanely chaotic and nontransparent,” he says. “The e-commerce companies that grew up in the boom who use e-mail almost exclusively are the canaries in the coal mine: E-Loan, Bizrate. And then there are existing companies who use e-mail a lot - Allstate & Geico [all Habeas customers]. There’s tremendous pain out there on the sending and the receiving side.”

He has raised $7.5 million from Diamondhead and Sky Moon on the strength of his evolving business model of increasing actionable information flow. The company currently has about 50 customers, including those mentioned (E-Loan, Geico,
Allstate, Bizrate) and also Webex, Homegain, Ziprealty, Tickle (now part of Monster.com), No-Ip.Com, Digital Mailer and Harris Interactive.

**CipherTrust: Meaning from the mess**

Another leading player in the e-mail hygiene field is CipherTrust. It keeps its reputation database, TrustedSource, as a proprietary benefit for its customers, who number about 1200. All told, estimates Paul Judge, CTO, its Ironmail gateway sits in front of 8.5 million inboxes.

However, CipherTrust does publicize the conclusions it draws from watching traffic for its customers, and is the industry’s go-to source. “We see about a million IP addresses a day,” says Judge, “and about a third of them are new each day.” That churn rate is why plain old lists of IP addresses and whitelists are simply inadequate for filtering the vast amount of mail that’s not easily classifiable. “We hope to use Sender ID to take our 95 percent success rate [in correctly identifying spam] up to 97 percent,” says Judge.

The company’s overall business model is selling its gateways to corporate customers (it has 30 of the Fortune 100), but like its peers, it uses its reputation database to gain visibility among prospects.

**Aligning the Incentives**

Most people still want mail to be free, both as in freedom of communication and in free of cost. But in fact, mail is not cost-free. All the processing of inbound mail described above is now costing large-scale mail services something around $8 to $10 per year per inbox. Moreover, they are not the people who should be paying those costs. In the most basic terms, the problem of spam is that costs and benefits are misaligned: Spammers send messages almost cost-free and gain some return from very low response rates; the recipients, both mail services and the ultimate individual recipients, bear the costs, both in money for filtering services and in user time and annoyance. Somehow, we must redress that balance. Goodmail is one early attempt to do so. (Vanquish, which we covered in July 2002, is another.)
Goodmail Systems: Making markets moral

While the other trusted-sender programs offer preferred rather than guaranteed delivery, Goodmail has spent the last 18 months and about $5 million of investors’ money to design TrustedClass E-mail – an explicit, sender-pays-per-piece service that will promise delivery to the user’s desktop, including (for most mail clients) a special icon that should induce the user to open the message once it is received. Call it FedEx for e-mail. (Indeed, if it gets too popular it will lose its impact, just as FedEx mail has. But that’s hardly a problem yet.)

The company was founded by its CEO Richard Gingras and Israeli entrepreneur Daniel Dreymann. Gingras has spent more than 20 years developing online services, including Apple’s eWorld, fussing constantly over user-friendliness and ease of use. While the best-efforts reputation-based warranting services work on probability and statistics for a mailstream, Goodmail’s TrustedClass E-mail is designed for mail that must get through to individuals – primarily customer service, transactions and account statements rather than marketing messages (though lots of vendors are also happy to pay extra for marketing, especially to known customers with good spending habits).

The service signs each e-mail with a digital “stamp” (i.e. signature), vouching for each individual message rather than just generally for a sender or a mailstream. The receiving mail server can ignore the stamp: I.e. stamped mail gets treated no worse and possibly better than regular mail by recipients who aren’t part of the program. But inbound mail servers that want to play can send the stamp code for each mail delivered to Goodmail and receive a substantial portion of the stamp value – which could range from 1/20 of a cent to a full penny per message. It’s unlikely any mail services will pass any of this revenue on to the individual recipients, but the Goodmail revenues may enable them to keep their prices down.

TrustedClass will include a number of other features to raise the ante: Each mail gets an added button for a recipient to report it as spam or to unsubscribe, so that there’s accountability for specific pieces of mail rather than for a sender’s overall statistical behavior. Currently, most users are reluctant to report spam directly, so they complain about it but not to the sender directly. That gives the sender a bad reputation, deserved or not, but does not give the sender any ability to remedy the situation even if that sender is really a (trying-to-be) good guy. The trail of accountability will be much tighter – and presumably, the user’s trust will be much higher. Says Gingras:
“It’s a closed loop. We handle the unsubscribes and make sure the feedback gets back to the sender about a specific individual’s preferences, not just as a number in a reputation database.”

In addition, TrustedClass-stamped messages (after a probation period for each sender) will show up with a special icon in the client mail systems of participating recipients (i.e. those who turn the stamps in for cash).

For the receiving mail service, all this will lead to greater user trust, service to the users (after all, mail services do want to deliver wanted mail reliably) and a little bit of revenue “to help cover the massive costs of e-mail hygiene they are bearing right now,” says Gingras.

All this, of course, is still just in the development stage. Because Gingras wants guaranteed deliverability, Goodmail can’t afford a best-efforts start-up phase. It needs to vet its sending customers carefully so that it will be able to get guaranteed deliverability for them. To keep using the service, senders must fall under strict limits of customer complaints—probably about 1 in 10,000, says Gingras. And it needs to work closely with its inbound clients, ISP’s and mailbox providers, who will be sharing in Goodmail’s revenues—to help them develop the tools to display the TrustedClass icons in their clients’ mailboxes.

Currently, Gingras won’t name any customers, but he does note that Goodmail has been working closely and collaboratively with some of the largest ISP’s and mailbox providers. This is an ambitious project. It has taken longer than Gingras originally anticipated...but by that very token, the achievement will be greater if it ends up working. The sheer difficulty of getting all the parties to work together—and of getting customers to trust their mail again—also represents a huge opportunity.

**Money meets mail**

We have long liked the concept of sender-pays (see **Release 1.0**, July 2002); Goodmail is a significant step in that direction. But in the end, sender-pays will work only if individuals or groups can set their own prices: That is, the receiver charges. At the same time, people are right to want to retain trust-based, best-efforts, nontransactional mail among peers who merely want to communicate, not to sell or buy.

That argues for some kind of two-tier system, under which individuals and small senders work with a sort of “deductible.” For example, a consumer e-mail account
could allow up to 100 messages a day - more than enough for most individuals (think cell-phone minutes). Goodmail hasn’t refined its precise terms yet, but it promises to provide some consideration for individuals and nonprofits.

On the other side, recipients will no doubt be developing their own whitelists of people whose mail they’ll accept for free beyond the people they know personally, but they will also be able to fine-tune filters and pricing for broader categories of incoming mail defined by their ISPs or inbound mail services. Their mail services may allow them up to some number of free inbound messages; beyond that, they’ll need to receive a certain level of paid messages, or pay themselves. We’re not sure how this would play out: The business model of people selling their individual attention to e-mail has not been successful (as opposed to sponsored content delivered on the basis of statistics). Ultimately, the volume of both “wanted” for a price and unwanted mail should go down, because senders won’t want to send to the kinds of people who are willing to receive (not necessarily read!) spam for pennies a message. (Advertisers don’t particularly like to pay to reach those people through broadcast media, either, but they do. That’s why they like “free” e-mail.)

As all these trends play out, sender-pays e-mail will start to look reasonable all around as a way to ease volume pressures and to provide a legitimate channel for legitimate marketing and for high-volume, high-value commercial communications. But at the edges of this paid market, there will probably be some kind of “free” or subsidized market.

And for that to work, there needs to be some sort of authentication system that keeps spammers from assuming mass numbers of small-guy identities. In other words, they should not be able to buy huge numbers of domain names or send huge amounts of mail without being accountable to someone. If we get both ISPs and domain-name registrars as well as mailing services into the accountable Net (below), that should be possible.

As for pricing, the pennies per message Goodmail will charge are too little to deter any determined marketer in the long run, but too much to bear for, say, a nonprofit mailing list or a nonprofit grandmother communicating with her family. The free-riders are willing to pay more than what seems reasonable to charge, and the good old trustworthy guys want things for free because they are good and trustworthy and that’s what they think they deserve. But in reality, even establishing yourself as good and trustworthy costs something - and in aggregate it costs a lot.
Hence the need for two markets. Ultimately price discrimination, not just pricing, will come into play. So, how can we get there?

The problem with spam right now is the sheer volume, which makes it tough to distinguish spammers from “regular” mailers. Meanwhile, processing payments by senders to individual recipients with individual pricing sounds like a crazy task in a world flooded with billions of mails a day. But if one did start charging per piece, with Goodmail succeeding to the point of attracting effective competition, the volume of messages would go down and the task of charging for them would become manageable - and funded. It will be some time coming, for sure, but eventually there’s likely to be a real market, where senders and recipients are properly matched.

More broadly, there’s a lot of posturing and inertia as we make the transition to a crass commercial market where everything has a price - though surely it’s much better than a crass commercial world without prices or ways for users to express their preferences. ISPs hate it when they hear an intermediary claiming that it (the intermediary) can promise delivery of mail…even though they have to pay attention to the reputation services as one of many factors in making filtering decisions. The reputation services claim they police their customers fiercely, but in the end their interests are misaligned: They are paid to help get the mail through, even though their long-term reputations (and profits) depend on their integrity.

Over time, the economic incentives need to be realigned.

Web Security: Who You Are

Spam in different flavors
Why do we care about spam? There’s spam that’s injurious because of sheer volume: It clutters up our inboxes and clogs the backbones; it distracts our attention from the mail we want and may make us miss something. But each single piece by itself is harmless (consider all arguments on this point incorporated by reference!).

Then there’s privacy-invading spam, which bothers some people and not others. They may not want to receive mail reminding them of their medical condition or their vulnerabilities; they may not want to be tempted to view porn or to buy a lovely pink sweater or a stuffed toy that will surely earn a loved one’s gratitude. Or they may not want to be reminded of something personal – by a friend or a stranger.
And finally, there's fraud and phishing spam and actual attacks – viruses and spyware downloaders and the like, and combinations of them. This is mail that can be specifically, objectively harmful, to the user's machine, her privacy or her pocketbook. This kind of mail may deliver a payload – technically or through social hacking – that compromises the user's machine. Or it may lure the user to a site where the user is induced to reveal confidential information or to download (inadvertently) spyware that can capture that information.

In other words, reducing spam is only part of the problem. The next issue is reducing vulnerability to fraud when a user is in actual communication with another party, either in response to an e-mail or just while on the Web. In such a situation, an individual user wants to know one or two things. First, are you the known site you say you are? And second, if you're unknown, is there a way to check your reputation? (We're not dealing here with issues of user authentication.)
We focus on the first question - authentication of an entity with a known reputation. Obviously, well-known institutions are the most likely to be spoofed – and the most broadly vulnerable to damage. Their challenge is that they may be able to establish secure communications with their customers, but they have a much harder time keeping their customers safe from third parties who may attempt to compromise the trust and security those established parties have built.

**Eudora 6.2: ScamWatch**

Inevitably, some spam will get through – and with it, some phishing invitations. Qualcomm’s new Eudora 6.2 includes ScamWatch (a name reminiscent of its MoodWatch and SpamWatch tools) to reduce the incidence of phishing attacks. Basically, it does something quite simple – but something most consumers don’t do for themselves. It checks that any URL within an e-mail that the user clicks on in fact matches the purported “name” of the link. (See Screen Shot, facing page.) “We’re looking for the basic disconnect of the text says X and the host you reach says Y,” says Eudora’s Bill Ganon, VP of Qualcomm Eudora Products. For example, the URL may appear in the message to be www.ebay.com/support, but in fact it’s 123.123.456.456. It would also catch, in a letter purportedly from eBay, www.ebay-support.com – a real URL, but not one registered to eBay. However, Scamwatch will not catch www.citicrop.com in a letter from Citicrop. (Read carefully!)

We like this tool and we think it’s handy, but it will provoke workarounds quickly as the Eudora 6.2 installed base grows.

**WholeSecurity: X-ray vision for the Web**

A bank wants to say: Don’t do anything with any site that you can’t positively identify as us. But how can it be there all the time to protect its customers? Into the breach comes WholeSecurity, which debuted at PC Forum last year. WholeSecurity launched its business with a secure communication service called Confidence Online; it helped a WholeSecurity customer such as a bank protect the security of its individual clients while they were communicating through the Web with that bank. Confidence Online can detect the presence of any kind of third-party spyware or Trojan horses that might compromise security, and then warn the consumer.

<table>
<thead>
<tr>
<th>WHOLESECURITY INFO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Headquarters: Austin, TX</td>
</tr>
<tr>
<td>Founded: August 2000</td>
</tr>
<tr>
<td>Employees: 70</td>
</tr>
<tr>
<td>Funding: $20 million from NEA, Venrock Associates, Trellis Partners and Parker Price Venture Capital</td>
</tr>
<tr>
<td>Key metric: revenues increased five-fold and number of customers grew from 10 to more than 60 from 2003 to 2004; customers include Deutsche Bank, Raymond James, Comerica, Cambridge Healthcare Alliance and eBay</td>
</tr>
<tr>
<td>URL: <a href="http://www.wholesecurity.com">www.wholesecurity.com</a></td>
</tr>
</tbody>
</table>
But of course, it couldn’t protect the consumer against doing business with Citicrop, or DetscheBank instead of DeutscheBank. “Companies are beginning to feel a more general responsibility for their customers,” says WholeSecurity CEO Pete Selda. So now WholeSecurity has a behavioral tool, Web Caller-ID, that checks the layout of the site an individual is visiting, compares it (for a fee from the “legitimate” site-owner) to the sites of commonly spoofed sites and brands, and watches whether it asks the user for compromising information – such as a social security number or other information that the user’s financial institution should already have (and should not be asking for). This behavioral approach, says CEO Pete Selda, is key. “We currently have over a 95 percent hit rate. Most of these phishing sites make most of their money in the first eight hours and disappear in a day or two. You can’t recognize them by signatures or a blacklist; you have to recognize them by their behavior.”
Web Caller-ID is also integrated into eBay's toolbar (a free service to its members) as part of its new (this year) AccountGuard feature – and WholeSecurity is working on similar arrangements with a variety of other well-known names. When a user protected with AccountGuard comes upon a suspect site, AccountGuard flashes up a warning and offers three options:

- Report this site.
- Close the browser.
- Go there anyway.

EBay has distributed WholeSecurity’s AccountGuard as a persistent, downloadable toolbar to 400,000 of its users. Of course, this has not gone unnoticed by the phishers, says WholeSecurity CEO Pete Selda: “The spoofers actually put a notice on the bottom of the spoof site: ‘If this site is flagged as suspicious by eBay AccountGuard, just ignore it. This is just a beta version.’ Of course, eBay and WholeSecurity warn

---

Source: Meng Wong
users against being taken in, but there’s just so much anyone can do against clever human engineering – and human vulnerability.

The challenge for the good guys is: How do you ensure that the customer is online with you only? You can make it secure while he’s online with you, but how can you keep him from mistakenly communicating with others? In the end, that requires a download of some kind (such as Web Caller-ID) - and the ability to make sure that some other download doesn’t masquerade by mimicking the particular “secure” sign that the user gets when he’s online with you.

The more tools such as Web Caller-ID are rolled out, the better off everyone will be. But the next step will be more accreditation and reputation systems for the little guys who are not as well-known.

The Accountable Net: Who Should Be Accountable?

In this issue, we have outlined some important steps towards making the Net more accountable, as mail service vendors and software companies come together to provide better tools and services to help individuals defend themselves against spam and fraud. However, the job is not done. IT vendors need to take on the tough and emotionally challenging task of educating their customers to be more careful. They need to sell systems with the security provisions turned on by default, even if that makes them harder to use and raises the volume of support calls. The costs of security need to be borne upfront, by users and by vendors giving up the competitive advantage of bare-bones pricing. Can security be sold to consumers as value-added? It’s tough, because vendors hate to mention any imperfections in their products. But the costs of insecurity, over the long run, will be even greater.

And there’s more. Two other sectors have a big stake in this online world but are mostly shirking their responsibilities. First, there are the Internet service providers, especially the cable companies who sell to home users and who don’t take care to support them properly, nor to watch for what kind of anomalous traffic may be coming out of their machines. A large proportion of spam is sent through the compromised machines of innocent (or at worst negligent) users. In the end, the companies that provide connectivity bear at least some responsibility for how it is used. In the long run, they, too, may suffer from blacklisting by peer networks if they don’t control their users. . .but wouldn’t it be nice if more of them would take
action before that is necessary?

But perhaps the most important group is the domain-name registrars, since they are the group that provide online identity. This is a highly competitive market (for which I bear some responsibility as founding chairman of ICANN, for Internet Corporation for Assigned Names and Numbers, the international organization that sets and to some extent enforces policy for the domain name system). Unfortunately, the competition is a race to the bottom; registrars compete primarily on price, since they add no value (such as reputation) and they can’t differentiate the product they sell – a domain name from a common registry. The idea some of us supported – sponsored top-level domains that would compete to provide meaningful distinction to holders of such names – has not been effectively realized. (The idea was that, say, .travel would be available only to travel companies that met certain rigorously enforced criteria, and that it would be promoted enough for consumers to take note of it. That’s still just an idea.)

As noted elsewhere in this issue, domain names (along with the e-mail addresses they support) are the main locus of persistent identity in cyberspace; they may be far too easily available. Originally, a domain name was a form of presence, a way to express oneself, and a medium for freedom of speech and information. But it is also, more and more frequently, a medium for collection of information (and money). How can we foster freedom without allowing fraud free rein?

The idea of a decentralized market is to have local regulation; but the domain name business seems to have no regulation and certainly little self-restraint. As Jon Callas, CTO of crypto provider PGP, says, “Both [the Sender ID Framework] and DK/IIM have to cope with people who set up domains that are ‘real’ domains in the reputation system. But – how are these spammers getting legitimate domains? Why, from the registrars, of course. Why aren’t we holding these people accountable? When someone registers the domain ‘drugs4u0000.biz’ through ‘drugs4u9999.biz,’ isn’t it pretty obvious that they are up to no good? Spammers are literally registering tens of thousands of throw-away domains per month. This is great revenue for the domain registrars. They’re profiting from the phishers. They are just as much part of the spam/fraud ecosystem as money launderers are part of the drug cartels.”
The premise for ICANN was to avert government regulation by introducing peer-to-peer regulation, not by having no regulation. But although most members would like to see their market cleaned up, no one can afford or is willing to go first. Because the domain name Juan's NobleName Registrar sells is the exact same domain name you could get from Alice's DeadbeatDomains, Juan can't afford to stay clean because the domain names he registers aren't associated with NobleNames. They're associated with, perhaps, “.com” or “.biz,” but nothing that's meaningful to a user. Unfortunately, the vision of competing registries of different TLDs with different and differentiable – extensions has not come to pass.

In short, the domain name system is not set up for accountability. It's not granular enough. There's one major registry for the .com Top-Level Domain (TLD) – VeriSign/Network Solutions – which leaves actual sales to customers to registrars. However, the registrars are not accountable: No one picks or avoids a domain name on the basis of the registrar that registered it. (And the hope that the new TLDs such as .biz and .info would be seriously differentiated and value-added has not been generally realized.) Since registrars are in principle the gatekeepers for the DNS, it's time they took on that role for real – or that ICANN allowed the creation of new, security-conscious TLDs that would deliver on a security promise.

The historical problem is that domain names are (supposed to be) open to all, but maybe a domain name is a privilege rather than a right – or at least a right that must be honorably, accountably used (e.g. having personal freedom vs. being sent to jail for a crime). Just like mailing services, the registrars need a way to get reliable feedback on their domain-holding customers. And like those mailing services, if they can't vouch for their customers, they may find themselves unable to sell services to them, since users will no longer go to those websites, just as they refuse the mail based on the overall record of a mailing service. The problem is that right now registrars aren't associated with the names they register (akin to the situation where you can't tie a message back to its sender). In fact, the whole structure of the domain-name market is based on the notion that you can get precisely the same domain name from any registrar, and there's no quality control.

Whether a new round of differentiated TLDs – with strong and well-promoted quality guarantees – would do the trick is open to question. But if the domain-name/website/web-hosting community doesn't learn pretty quickly from the kinds of reputation systems that the mailers are beginning to use, they may face more draconian forms of feedback – such as government regulation.
Hold tightly to the hand of nurse, for fear of finding something worse

Thus, back to the accountable Net. Unregulated by government does not mean completely unregulated. In theory, the government should be regulating the behavior of all the entities on the Net. We don’t believe government is up to that task. But we do believe that the entities on the Net can regulate one another, if systems are set up properly. And they have an interest in doing so.

Real reputation-based and quality-controlled competition among TLDs would be not a solution to everything, but it would be one more important step towards cleaning up the Net. Either those who use domain names need to be accountable to those they interact with, or those who register the domain names need to be accountable for them, in a way visible to individuals and the public. This accountability needs to be specific and granular, so that one can separate the good from the bad. Otherwise, the public will hold the Net as a whole accountable for the actions of its malefactors.
Resources & Contact Information

Michael Barrett, American Express, 1 (602) 537-2529; michael.barrett@aexp.com
Susan Crawford, Cardozo Law School, 1 (212) 790-0493; scrawford@scrawford.net
Paul Judge, CipherTrust, 1 (678) 904-9152; pjudge@ciphertrust.com
Jennifer Martin, CipherTrust, 1 (678) 904-9151; jmartin@ciphertrust.com
John Noh, Cisco Systems, 1 (408) 853-8445; jnoh@cisco.com
Dave Rossetti, Cisco Systems, 1 (408) 527-3777; rossetti@cisco.com
Jen Schwartzman, FTC Office of Public Affairs, 1 (202) 326-2674; jschwartzman@ftc.gov
Richard Gingras, Goodmail Systems, 1 (650) 230-7777; fax, 1 (650) 230-7801; richard@goodmailsystems.com
Des Cahill, Habeas, 1 (650) 694-3312; fax, 1 (309) 405-7742; des@habeas.com
Scott Banister, IronPort Systems, 1 (650) 246-8980; sbanister@ironport.com
Scott Weiss, IronPort Systems, 1 (650) 989-6520; sweiss@ironport.com
Ryan Hamlin, Microsoft, 1 (425) 882-8080; ryanh@microsoft.com
Jon Callas, PGP Corporation, 1 (650) 319-9016; fax, 1 (650) 319-9001; jon@pgp.com
Bill Ganon, Qualcomm, 1 (858) 651-0009; fax, 1 (858) 658-1220; bganon@qualcomm.com
Dave Anderson, Sendmail, 1 (510) 594-5401; davea@sendmail.com
John R. Levine, Taughannock Networks, 1 (607) 330-5711; info@taugh.com
Fran Maier, TRUSTe, 1 (415) 520-3418; fran@truste.org
Scott Olson, WholeSecurity, 1 (512) 874-7449; scott.olson@wholesecurity.com
Pete Selda, WholeSecurity, 1 (512) 874-7439; pete.selda@wholesecurity.com
Brad Garlinghouse, Yahoo!, 1 (408) 349-5783; bradg@yahoo-inc.com

For further reading:
Overview of Sender ID: http://www.microsoft.com/mscorp/twc/privacy/spam/senderid/overview.mspx
Cisco comments to the FTC on e-mail authentication: http://www.ftc.gov/os/comments/emailauthentication/512447-0032.pdf
Summary, Accountable Net Roundtable, Cardozo School of Law, June 2004: http://scrawford.net/courses/accountablenetroundtable.doc
PPT Deck that details How Sender ID works:
SPF Classic: http://spf.pobox.com
Cisco’s Identified Internet Mail: http://www.identifiedmail.com
World Wide World: IT ain’t just the Web anymore!

The World Wide World of the Web is now extending beyond IT. We’re expecting IT to solve real-world problems, even as real-world problems affect our use of IT.

IT is helping to solve social problems (medicine, education, security) as well as business challenges (supply chain management, customer relations, sales and marketing, regulatory compliance). But we need to solve real-world problems in order to use IT - many of them the same ones that IT can help solve: education, employee motivation, health-care costs, economic dislocations and the like. How is IT changing real-world business models, and how are IT’s own business models changing as customers supply more of the value, as open source erodes margins and as more and more value is delivered as intellectually enhanced services?

This year, more than ever, you can have fun at PC Forum and be productive at the same time. The mood will be upbeat because our industry is recovering, and even outsiders recognize the value of IT (!). Better yet, they need our help to make it work. At PC Forum, we’ll look at the wide world around us through the lens of information technology in a useful way. You’ll hear about new technologies and new companies and how they will affect your business as well as the world around you; you’ll understand the strategic gyrations of the big players; you’ll test your ideas against those of others on the panels and in the hallways; you’ll meet the potential partners and competitors that form your community at the social events.

IT leaders and business leaders – and you – will have the chance to share and challenge one another’s assumptions about what works in the real world. IT alone isn’t enough: More and more of the value of IT depends on how the customers make use of it. We’ll also assess corporate IT initiatives, as users strive to differentiate themselves with custom software to create strategic advantage. Where does that leave traditional application vendors?

In our increasingly friction-free world, good ideas don’t differentiate you for long. How can businesses use IT more effectively to serve their customers, and to differentiate themselves?

Invited speakers include: Marc Andreessen Chairman & Co-founder, Opsware; Claiborne Barksdale, CEO, Barksdale Reading Institute; *Jeff Bezos, Chairman, Amazon.com; Sergey Brin, President, Technology & Co-founder, Google; Howard Gardner, Professor of Cognition and Education, Harvard Graduate School of Education; Jeff Hawkins, Chairman & Executive Director, Redwood Neuroscience Institute; Dawn Lepore, CEO, Drugstore.com; Robin Li, CEO, Baidu.com; Anne Mulcahy, Chairman & CEO, Xerox; Marjorie Scardino, CEO, Pearson; Jonathan Schwartz, President & COO, Sun Microsystems; *Martin Sorrell, Chairman, WPP Group; John Thompson, Chairman & CEO, Symantec; *Ed Zander Chairman & CEO, Motorola.

Join us and the World Wide World at PC (Platforms for Communication) Forum 2005

To register and for more information, please visit http://www.pcforum2005.com

*awaiting confirmation
Visit our new website: More (free-to-read) columns, ideas, essays, features and contributors...featuring Rafe’s Radar, a biweekly column by Rafe Needleman. Plus, a new look!

http://www.release1-0.com

Release 1.0 Subscription Form

Complete this form and join the other industry executives who regularly rely on Release 1.0 to stay ahead of the headlines. Or if you wish, you can also subscribe online at www.release1-0.com.

Your annual Release 1.0 subscription costs $795 per year ($850 outside the US, Canada and Mexico), and includes both the print and electronic versions of 11 monthly issues; 25% off the cover price when you order from our online archives; a Release 1.0 binder; the bound transcript of this year’s PC Forum (a $300 value) and an invitation to next year’s PC Forum.

NAME

TITLE COMPANY

ADDRESS

CITY STATE ZIP COUNTRY

TELEPHONE FAX

E-MAIL* URL

*personal e-mail address required for electronic access.

☐ My colleagues should read Release 1.0, too!
Send me information about multiple copy subscriptions and electronic site licenses.

☐ Check enclosed ☐ Charge my (circle one): AMERICAN EXPRESS MASTER CARD VISA

CARD NUMBER ________________ EXPIRATION DATE ________________

NAME AND BILLING ADDRESS

SIGNATURE

Please fax this form to Brodie Crawford at 1 (212) 924-0240.

Payment must be included with this form. Your satisfaction is guaranteed or your money back.

If you wish to pay by check, please mail this form with payment to: EDventure Holdings, 104 Fifth Avenue, 20th Floor, New York, NY 10011, USA. If you have any questions, please call us at 1 (212) 924-8800; e-mail us@edventure.com; www.release1-0.com.