From the Editor in Chief...

On Social Networking and Communication Paradigms

Fred Douglis • *IBM T.J. Watson Research Center* • *f.douglis@computer.org*

First off, I wish all readers of *IC* a happy and healthy new year. We traditionally rotate our tracks at the start of the year: for 2008, K.J. Lin and Yan Wang are editing one on e-commerce (see p. 60 for an introductory piece), and M. Brian Blake and Mike Huhns will be covering Web-scale workflow (see p. 55). We also introduce new (and remove older) columns around this time: Stephen Farrell tests out a new column on practical security (p. 93), and you'll note that the "From the Newstand" department is no longer featured in the magazine.

Finally, my colleague Barry Leiba at the IBM T.J. Watson Research Center has taken over the Internet Standards department that Jim Whitehead managed for us for several years. Jim has our deepest thanks for his efforts. Although Barry will cover a range of standards in the department — he starts with an overview of what he will be looking at on p. 71 — his own area of research is one near and dear to me: combating email woes, such as spam. His column this issue discusses several proposed standards for identifying when the sender of email has been forged, but I'd like to touch on several other aspects of this problem myself.

Mail Fraud

My last two columns shifted from the general theme of "What can we do about those rotten spammers and scammers?" to "What can we do about the lack of integrity in the academic publishing process?" (I discussed detecting self-plagiarism in the September/October 2007 issue and rating reviewers in the November/December 2007 one.) I now return to my tried-and-true theme (also known as "What bugs Fred?").

First, let's start with a premise that few people will disagree with: email is broken. Huge portions of all email are spam. As a systems person, I can readily believe that "email 1.0" was nice and open and trusting because it was easy, and its early adopters had little to worry about from miscreants, who wouldn't really come online for a decade or two. But I have trouble accepting the premise that we've failed to migrate the Internet to an "email 2.0" that would fix all the problems. The larger mail sites have made some progress on identifying when mail doesn't originate from the domain claimed in its header (again, see Barry's column this issue), and I know some chicken-and-egg issues and critical-mass issues have to be addressed for any fix to take off. However, by and large, things are badly broken, and the basic protocol is the same broken one we've been using for years.

Example 1

I find that mail from one of my domains doesn't reach some recipients and only occasionally results in a response that indicates any problem exists. (Presumably, this occurs because that particular IP address is incorrectly being blacklisted as a spam sender, something that every few months prevents it from forwarding messages to the ISP where I used to read my mail. After two such outages, I started reading my mail on Gmail.) Thus, the identification of suspect domains and the throttling of email from those hosts can easily sweep legitimate mail into the net of suspect behavior. Recently, I even found that mail from my work address at IBM to a particular university came back unread because the IP address from which it was ultimately forwarded outside IBM had been blacklisted. Individual users shouldn't have to worry about whether their ISP is getting a "bum rap"

 1089-7801/08/$25.00

like this. And when mail is dropped or delayed, it would be awfully nice to know about it — if and only if I legitimately sent it in the first place.

Example 2

As I mentioned in my March/April 2007 column, I get huge amounts of mail to addresses on my domain that don't actually exist, almost all of which are bounces of mail that purported to come *from* these bogus addresses. Although an invalid address is easy to catch, once in a while I get a flurry of bounces that come from a legitimate return address. Unless I'm willing to ignore bounces of mail that I actually sent, I must skim these messages (or at least the first couple) to see if they're legitimate. (Barry pointed out that a proposed solution to this is to provide a cryptographically signed returned address to which to send bounces of legitimate mail; you could then ignore bounces to mail others have spoofed. See http://mipassoc.org/batv/ for more information about Bounce Address Tag Validation [BATV].)

Example 3

Five years ago, Slate.com published an article by Kevin Werbach entitled "Death by Spam: The E-Mail You Know and Love is about to Vanish" (www.slate.com/id/2074042/). The argument at the time was that whitelists, in which users accept mail from certain known senders and reject everything else, were inevitable. He described email as becoming similar to instant messaging "buddy lists" in which people communicate among closed circles. A few days ago, I listened to a podcast of a new *Slate* article by Chad Lorenz, "The Death of E-Mail: Teenagers Are Abandoning their Yahoo! and Hotmail Accounts. Do the Rest of Us Have To?" (www.slate.com/id/2177969), which made a related point. It said that teens are switching to other media such as social networks, blogs, and broadcasts (such as Twitter) in preference over email. The net effect is to make communication among known associates much more prevalent and convenient than among strangers.

Unintended Consequences

In my last reference to Barry's writings, I will mention his recent blog entry (http://staringatemptypages.blogspot.com/2007/11/more-on-social-networking-sites.html) about the dangers of social networking sites lulling users into a false sense of security. He cites work by Aaron Zinman and Judith Donath,[1] as well as a posting on *The New York Times* blog (http://bits.blogs.nytimes.com/2007/11/08/hackers-infect-alicia-keyess-myspace-page/index.html), both of which describe the use of social networking sites by spammers and those who wish to trick users into downloading malware. The gist of these items is that if users are accustomed to downloading and installing software when they visit pages on these social networking sites, they can easily be duped into doing something they've finally become careful about in the context of email. (See also the article on social networking spam by Paul Heymann and colleagues in last month's issue.[2])

Putting together the ideas of whitelisting known good senders, the poor detection of forged senders, and the increasing prevalence of social networking, I can reach only one conclusion. If we can't trust email messages' senders to be who the notes claim they are, then whitelists are doomed: the increasing visibility into end users' social connections will make it easy for scammers to figure out just what return address to forge! Up to this point, it hasn't been important enough to spammers to customize addresses like that; aside from phishing attempts — which claim to be from a vendor that a recipient might or might not actually have a relationship with — the sender could be anyone. But if I started getting email from my *wife* saying "check out this site," it might get my attention. What's next, a password-of-the-day?

Social networks are an amazing phenomenon that offer numerous new opportunities compared to more traditional environments such as email. At the same time, they've been adopted in large part by many of the most inexperienced and naïve users (teenagers, although I grant that some teens are far from naïve). Let's get our defenses correct early in the process, lest we fall prey to the same hardships that SMTP encountered. The purveyors of social networking infrastructure have to be particularly diligent in this regard. Policies such as Google's orkut system that let strangers write in my "scrapbook" led me to drop my account when the

IC Welcomes a New Board Member

Carole Goble is a full professor in the School of Computer Science at the University of Manchester, where she co-leads the Information Management Group. She is also the founding chair of the multi-organizational Open Middleware Infrastructure Institute–UK. Her research interests include the application of information and semantic technologies, such as ontologies, to data-intensive applications, particularly e-science, and specifically the life sciences. Goble was the co-PC chair of the World Wide Web Conference in 2006, and is the editor in chief of Elsevier's *Journal of Web Semantics*. She serves on more than 15 boards and committees, including the Semantic Web Science Association and the Web Science Research Initiative Scientific Council, and has given keynotes in most of the major conferences in her fields.

only activity was the frequent appearance of spam. More recently, Facebook has suffered criticism for revealing private shopping information about its users in an "opt-out" fashion (see http://civ.moveon.org/facebookprivacy/071120email.html).

Email and social networks aren't the only communication paradigms under assault. Despite "junk faxes" being illegal in the US for many years, I continue to get several a week at home. Some postulate that a new threat is *spam via Internet telephony* (SPIT). Although I've received telemarketing calls at home (thankfully very few since the enactment of the US's "do not call" registry), I've received only one or two junk calls on my cell phone, most likely because not only are such calls illegal, the originator is easily traceable. But it's probably only a matter of time until SMS spam and IP-phone junk calls are commonplace, unless we initiate appropriate safeguards. Alternatively, we'll move to whitelists restricting who can call us, who can send us text messages, and so on — and people with legitimate reasons for access will inevitably be turned away in the process. (P.S. Within days of writing the first draft of this column, I received two spam messages on my cell phone and had to research exactly how to set up the whitelist.)

Acknowledgments

Thanks to Barry Leiba, John Tracey, and Zhen Xiao for helpful comments and suggestions. The opinions expressed in this column are my personal opinions. I speak neither for my employer nor for *IEEE Internet Computing* in this regard, and any errors or omissions are my own.

References

1. A. Zinman and J. Donath, "Is Britney Spears Spam?" *Proc. 4th Conf. Email and Anti-Spam*, 2007; http://smg.media.mit.edu/papers/Zinman/britneyspears.pdf.
2. P. Heymann, G. Koutrika, and H. Garcia-Molina, "Fighting Spam on Social Web Sites: A Survey of Approaches and Future Challenges," *IEEE Internet Computing*, vol. 11, no. 6, 2007, pp. 36–45.