

Miracle Cures and Toner Cartridges: Finding Solutions to the Spam Problem

Panel Moderator: Michael Clifford
Associate Member of the Technical Staff, The Aerospace Corporation
clifford@aero.org

Panelists: Daniel Faigin
Engineering Specialist, The Aerospace Corporation
faigin@aero.org

Matt Bishop
Associate Professor, The University of California at Davis
bishop@cs.ucdavis.edu

Tasneem Brutch
Information Protection Consultant Specialist, Kaiser Permanente
tbrutch@ieee.org

Panel Theme

The exponential growth in unsolicited commercial e-mail, or spam, over the past several years has resulted in a degradation of e-mail as a useful medium for information interchange. Spam traffic wastes resources, drives up costs for access providers, and imposes a high social cost. Spam filtering systems often delete legitimate e-mail, resulting in a loss of e-mail as a reliable method of communication. Additionally, the lack of strong authentication in the current e-mail system provides a mechanism by which spammers can trivially spoof both their own identities, and the identities of the hosts that they used to send their spam. Because spoofed addresses often point to real accounts, the legitimate owners of these accounts often lose access to their own mail services when the recipients of spam send messages to those accounts trying to move themselves from a spammer's mailing list.

In many respects, spam could even be considered a denial of service attack against the entire Internet. As such, it represents a security issue not unlike those that typically face hosts and networks. Many possible solutions have been proposed to this problem, including government regulation of e-mail, the use of micropayments for e-mail transmission, low-level redesigns of the current mail transport system, the application of trust and authentication models, and the use of computationally intensive puzzles. Each of these possible solutions has a variety of advantages and disadvantages, although none appears to be a perfect

solution. This panel will explore the problem of spam from a security perspective, whether or not e-mail should be regulated in some way to prevent spam, which, if any, of the proposed solutions should be adopted, and how such solutions could be deployed throughout the Internet given the presence of a pre-existing e-mail infrastructure.

Position Statements

Daniel Faigin

Spam is a clear security issue for systems: it creates privacy risks through web bugs; creates the risk of spreading worms; and is a clear availability attack for mail servers as well as end user time. Many have proposed various solutions to the problem of spam, from government regulation to software approaches to the redesign of software and protocols. I believe that none of these will work, for a variety of reasons. First, it is difficult to identify spam. Spammers are clever, but more importantly, what is spam to some may not be spam to others. This prohibits technological approaches, although the Bayesian filters in use by products such as SpamAssassin work well... most of the time. Legal approaches are possible, but don't work well and are hard to enforce, due to the international nature of the Internet.

So what is the answer? Consider that only a small percentage of spam is read, and a smaller percentage garners a response. But as long as there are responses, and the profit made by those responses justifies the time spent, there will be spam. The answer is economic. By an

intense education effort, we must teach people to delete spam unread. Scan the headers and press the "D" key. Don't even open it up. This eliminates the security risk, and the economic effects will reduce the availability attacks. If the spammers learn that this method of advertising is unprofitable, they will move to more profitable methods.

Tasneem Brutch

Spam, also known as Unsolicited Commercial Email (UCE), or Unsolicited Bulk Email (UBE), is currently one of the bigger nuisances on the net, and has reached levels where it is starting to interfere with the effectiveness of email as a communication medium. It has gone from being annoying, distracting, and irritating, to being expensive. One of the more significant issues with spam, is that the sender pays very little of the cost per message, such as the time and cost of setting up an account with an ISP. The host relaying the mail pays for most of the cost of transmission, in bandwidth, service degradation, and the expense of responding to complaints, to name a few. In addition to the mail relaying host, the system targeted by spam pays in bandwidth loss, connection expense, unnecessary disk usage, over-flowing user mail boxes, and loss in productivity. Recipients of spam have to spend time to sort, read, and delete unsolicited and unwelcome messages. The cost of lost productivity due to Spam, is about \$1 billion/year. Such a significant loss in revenue and time, can likely decrease user confidence in the use of e-mail as an effective medium of communication.

The security implications of spam are both significant and disconcerting. Even wireless phones with text capability are becoming targets. Apart from costing corporations billions of dollars in lost productivity and resources, it is a theft of resources. It steals the resources of the recipient network by consuming bandwidth, and by taking up space on mail servers. Servers receiving emails are overwhelmed by the sheer volume, which may result in denial of service for legitimate users. Either intentionally, or unintentionally, Spam can be the carrier for computer viruses and malicious code. In some cases, JavaScript embedded in e-mails contains flaws, and result in crashing the e-mail application and/or the system, resulting in unnecessary time and effort needed for system recovery by users and system administrators. AOL has estimated that spam constitutes up to 30% of all incoming emails on its networks. Brightmail reported that 36% of all email on the internet in July 2002, was unsolicited. From the perspective of ISPs, the large amount of data flowing through the networks makes it difficult to implement a comprehensive solution to secure networks against spam, and prevent this form of network abuse.

Whenever possible, the decision pertaining to what an end user would like to see, should be made by the end user receiving the email. Academic institutions that wish to limit the amount of spam coming into their networks, have to balance security and functionality. Educational institutions also need to consider freedom of speech issues and First Amendment rights, when dealing with spam. Efforts to curtail spam should be multi-layered. Spam can be targeted with improved federal and international laws. Content filtering and blacklists can be used, along with e-mail gateways, and corporate e-mail policies to fight spam at the network level. In addition users should be educated to fight spam at the workstation level. Legislation and regulation alone cannot completely curtail spam. Email software vendors should incorporate anti-spamming capabilities into their software. Enough economic and legal disincentive should be there to make spam cost prohibitive for the sender, with associated penalties.

Matt Bishop

Spam is defined as "bulk unsolicited email". This has two elements: "bulk" and "unsolicited". What exactly do these terms mean?

Suppose I send a friend a letter extolling the benefits of Dr. Quackenbush's cure for which there is no disease? That is clearly not spam, by the above definition. Suppose I send it to 10 friends? 50? 500? 5000? At what point does what I send become "bulk" email?

Now consider "unsolicited". Some aspects are clear: if someone harvests names from USENET postings, for example, and sends advertisements to those addresses, that's spam. But suppose I sign up for a mailing list, and allow it to circulate my name. A vendor acquires my name from that list and sends advertisements to many people, including me. Is that spam? Must I explicitly allow the list owner to circulate my name to "solicit" email, or can the list owner assume I allow this implicitly?

In short, spam can overload system resources making those resources unavailable, and the reaping of addresses can violate peoples' privacy. This suggests a definition of spam along the lines of security, a definition phrased in terms of the objectionable characteristics, just as security is defined in terms of forbidden states (by a security policy). If I receive 100 e-mail advertisements per hour, and those advertisements are targeted explicitly at me, and no-one else, that is objectionable. But by our current definition, that's not spam.