JOURNAL OF OBJECT TECHNOLOGY

Online at http://www.jot.fm. Published by ETH Zurich, Chair of Software Engineering ©**JOT, 2004**

Vol. 3, No. 1, January-February 2004

On The Spam Scourge

Won Kim, Cyber Database Solutions, Austin, Texas, U.S.A.

1 STATUS

By now email has become an indispensable means of communication for mankind. However, during the past few years, it has been hijacked by spam. A resounding majority of email users are very much annoyed by their daily struggle with spam. They are forced to glance through a large number of unwanted, misleading, or offensive emails from out of nowhere; they have to purge from the inbox and deleted box somewhere between 50 to 80 percent of their incoming emails every day; and they often mistakenly purge some important emails. The cost of spam is borne mostly by individuals, and corporations that end up transmitting and receiving spam. It includes the cost of computers, disk storage, and networking equipment, as well as all the time the receivers waste.

During the summer of 2003, I came to notice that about 80 of 100 emails I received a day were spam. Most of the spam was in English and Korean (I hold a professor position in Ewha Women's University of South Korea, while running a consulting business, Cyber Database Solutions, in the US, and managing the ACM SIGKDD international academic society and the ACM Transactions on Internet Technology international scholarly journal.). Some of the spam was in foreign languages that I do not even know. I realized that my email address had been "harvested" by master spammers from my two business websites, the university website, the society website, the journal website, the website of the conference the society runs, etc. Further, in the past, I had too readily given my email address to all IT trade publications that offered free subscription, and I suspect some of them may have sold the email addresses of their subscribers to various businesses, which in turn have sent me spam. I installed a spam filter, but I quickly realized that it did not really solve my spam problem since I had to scan all emails the spam filter threw into the spam folder to "de-filter" erroneously filtered emails. So, I took a drastic measure. I abandoned my single "universal" email address. I created five different email addresses, each for different function and purpose – one for communication with Ewha University, two for my business, one for ACM, and one for friends around the world for non-business communications. Should my email address get hijacked again, I did not want to abandon the email address again and have to notify everyone who communicates with me via email. I wanted to only notify a segment of my "email communication partners". Also, I had my "ACM" email address encoded in the SIGKDD and TOIT websites. I still receive some spam – several a day through my Ewha

Cite this column as follows: Won Kim: "On the Spam Scourge", in *Journal of Object Technology*, vol. 3, no. 1, January-February 2004, pp. 55-59. http://www.jot.fm/issues/issue_2004_01/column5

Women's University email address, a few a week through my "friends" email address. But now I feel that my life is back in order.

The primary culprit of the current scourge of spam is about 200 "master spammers" who send out millions or even tens of millions of emails a day, peddling a wide range of products and services, including generic Viagra, ink jet printer cartridges, diet solutions, male body-part enlargement medicines, etc. Master spammers take a cut of the sales made on the products and services they brazenly "mass market". The next major culprits are the "legitimate" businesses that promote their products and services by sending emails (without hiring master spammers or acting like master spammers) to a list of email addresses they acquire. Further, every day lots of individuals send emails to a large number of people needlessly, such as "I am mad at the lousy service I received from my car dealer today, so I urge you all in my company not to buy a car from that dealer".

2 CURRENT APPROACHES

The spam problem really must be solved somehow and soon. Today, despite the very widespread unhappiness on the part of email users and the staggering cost it incurs, spam does not show any sign of coming under control. So far, basically three types of approach have been used to combat the spam scourge. First is technology. There are lots of spam filters on the market. Internet service providers try to block email servers that appear to have been used as sources of spam. Further, since master spammers use software to automatically "harvest" email addresses from public websites, now webmasters have taken to encoding email addresses that appear on their websites. The spammers and spam filter vendors and Internet service providers have been engaged in a continuously escalating game to outsmart each other, and there are no clear signs that the spammers have given up. Second is legislation and law enforcement. This has been a disaster area. Only a small number of spammers have been prosecuted for "using other people's properties (computers) without authorization" to route their emails. Although the US Congress has recently passed the Can-Spam Act to make spam illegal, not many believe that the Act will stop the master spammers. Third is vocal and strong complaint from some of the people who feel fed up by spam and who try to "spam back" the spammers with vociferous and even (justifiably) abusive reply emails. Some master spammers have confessed that it is "not easy to stay ahead of the technological solutions being put up by the Internet service providers and spam filters, and to take 'nasty replies' from the 'masses' they bothered". In fact, it is the loud expression of frustration and anger from many email users that has led to the government actions on spam thus far.

3 WHY CURRENT APPROACHES HAVE NOT SUCCEEDED

There are several reasons spam has proven to be a very difficult animal to tame. First is availability of spam-aiding technology. Spammers use software to harvest email addresses from public websites and to automatically generate random email addresses (to get to 'wonkim', they tried 'wonderboy, wonderman, wonderwoman, wonderk,….'). Spammers also use software to crawl the Internet to discover computers that they can use as proxies and relays to send and route spam through. Second are technological shortcomings. It is very difficult to trace spam back to the spammers, especially so because they, again using software, camouflage their sender identities (I have received spam 'From' wonkim 'To' wonkim). Spam filters cannot guarantee zero false positives and zero false negatives, especially when spam arrives often with such innocent Subject lines as "lunch?", "confirmation", etc. The holes in spam filtering force email users to examine all emails in the spam box to discover any false positives. Third is obstruction from "legitimate" corporations. (Although these days it is not easy to define 'legitimate' corporations, I will try to give a simple working definition later in this article.) Many "legitimate" corporations fear that any law that makes spam illegal will be used to prevent them from being able to send promotional emails. Fourth are the inadequate laws. Not all spammers are based in the United States. Many in the United States hijack or otherwise use computers in China and elsewhere. Some spammers are teenagers. Some spammers offer the "Remove" button, but do not actually remove people from the mailing list. Existing laws do not even make clear what constitutes "fraudulent" email. Some spam do not lend readily to complaints – "enlarge a male body part", "marry a beautiful Russian woman", "lose weight while sleeping", etc. Fifth is the difficulty of enforcement. Law enforcement agencies are busy enough to fight terror, deal with conventional offline crimes, respond to emergency calls, etc. People resources needed to track down spammers and bring them to "justice" are seriously inadequate in number and training.

4 MY OPINIONS

In view of the difficulties that existing approaches have had, there have been a few new suggestions of late for combating spam. One is to charge a "tiny" fee for every email anyone sends. The amount would be negligible for most "innocent" email users. However, for a master spammer who sends out millions of emails a day, the fee can quickly add up and eat away a big slice of his profits. This is the seed of a good idea, and I will discuss shortly how this may be extended to what I think is something more solid. Another suggestion is, before delivering to final destination, to send a suspected spam mail back to the original sender and have the email wait until some time-consuming computation is completed, and then allow the email to proceed as a normal email. I do not think this idea solves any problem. This will simply delay delivery of spam. Finally, in connection with both the legality and automatic blocking of emails, there are the ideas of "opt in and opt out". The "opt in" idea is that an email should be delivered only to the users who have explicitly agreed in advance to receive emails from the sender. The "opt out" idea is that an email should be delivered to any user as long as the user has not explicitly requested to not receive emails from the sender.

Now I would like to offer some simple suggestions to solving the spam scourge. The biggest challenge is to stop master spammers. I think a two-part approach should be taken. The first part is to make it illegal for businesses (or individuals engaged in a business act) to send emails to anyone who has opted out or who has not opted in. This would set the legal basis for the second part, which is to hold both the spammers and the advertisers liable and be made to pay a staggering penalty. The Can-Spam Act is the first legal step necessary. However, it falls short by not making advertisers liable. Master spammers are not sending out millions of emails a day to have fun or to cause mischief; rather, they want to make a lot of money by doing it. Advertisers pay them a slice of the sales. In other words, these people work on “mass marketing” contracts from the advertisers, and the advertisers should be compelled to be responsible for the actions of their contractors. Besides, advertisers are likely to be less “mobile” than technologically savvy and determined master spammers, and so should be relatively easier to catch and bring to justice. It is of course necessary to have laws in order to drive master spammers and their clients out of business (at least as practiced today by bothering practically the entire mankind). However, it is absolutely essential that the laws be enforced vigorously. The government should train and deploy sufficient human resources to monitor compliance, track down spammers, and prosecute them.

The next biggest challenge is to stop “legitimate” corporations from launching spam. In light of the accounting shenanigans that apparently many “legitimate” big corporations have engaged in for some years, and the thousands or tens of thousands of bugs that lurk behind most complex software products on the market these days, the distinction between “legitimate” corporations and ‘illegitimate” corporations does not appear cut and dried. For purposes of this article, I will simply define a “legitimate” corporation as one which sells products and services that work to a good extent as advertised, and which will not send promotional emails to people who do not want to receive them. Such a corporation would likely send promotional materials only to people who are on their lists of customers, partners, attendees in their User Conferences, etc., and promptly honor opt-in and opt-out requests from people. Many legitimate corporations may often outsource tactical marketing, such as email-based promotional campaigns, to third-party firms, just as various shady advertisers outsource their promotional campaigns to master spammers. However, most legitimate corporations tend to have their own marketing staff and conduct promotional campaigns on their own, rather than outsourcing them to third-party firms. This can help prevent corporations from erecting a wall between them and third-party marketing firms, and trying to pin the blame on the third-party marketing firms for any spam-related liabilities. However, I believe such legitimate corporations should be charged some non-trivial fees for promotional emails they send. The volume of such emails tends to be relatively large (although nowhere near what the master spammers today cause) and as such they burden the Internet and Internet service providers. If email-based promotional campaign is entirely free, they may be tempted to be more indiscriminate. Besides, email users are likely to be interested in only a small fraction of the emails they receive from these corporations, and be bothered by the rest of the emails. This situation is no different from all the (hardcopy) junk mails people receive (and toss to the trash cans after one quick glance) from the businesses they shop and deal with, such as department stores, car dealers, computer stores, supermarkets, banks, insurance companies, etc. The senders pay to send such junk mails rather indiscriminately. It appears that legitimate corporations really should pay to send "junk" emails.

The third source of spam is what I would loosely call emails that the great majority of email users, the "ordinary" users with nothing to promote (except for themselves), send needlessly or carelessly to uninterested or inappropriate parties. Perhaps these should be more aptly and charitably called junk email, given their much less ferocious nature and impact compared to what master spammers generate. There is no technology and no law that can or should stop people from sending emails to people who do not need to receive them. People will always make mistakes in judgment, mistype email addresses, get upset and send flames to a bunch of people needlessly, etc. People generally do not pay attention to the fact that all emails are being sucked up by systems operated by government intelligence agencies, such as the NSA's Echelon and the FBI's Carnibore; and that they are stored on disk along the route between the sender's computer and the receiver's computer. The US Department of Justice used such stored emails from Bill Gates to certain people to prosecute its anti-trust case against Microsoft several years ago. As people misuse emails and pay a price for doing so, they will become more cautious about sending needless emails. Despite such tempering that comes with experience, however, the problems of needless email traffic that people generate will continue to grow, as more and inexperienced people become email users, and as people rely on emails more, increasingly with multimedia attachments.

About the author

Won Kim is President and CEO of Cyber Database Solutions (http://www.cyberdb.com/) and MaxScan (www.maxscan.com) in Austin, Texas, USA. He is also Dean of Ewha Institute of Science and Technology, Ewha Women's University, Seoul. Korea. He is Editor-in-Chief of ACM Transactions on Internet Technology (http://www.acm.org/toit), and Chair of ACM Special Interest Group on Knowledge Discovery and Data Mining (http://www.acm.org/sigkdd). He is the recipient of the ACM 2001 Distinguished Service Award.