

You Have Spam!

How to prevent your machines from being used to
advertise get rich quick schemes, Asian
prostitutes and off-shore gambling.

Michael D. Sofka

Computing Information Services
Rensselaer Polytechnic Institute

Slide 1 Upstate New York Systems Administrators Guild
April 1, 1999, Rensselaer Polytechnic Institute

`sofkam@rpi.edu`, `http://www.rpi.edu/~sofkam/`

Notes for slide 1:

- Imagine you are the administrator of the mail machine at a mid-sized college.
- Or, if not **the** administrator, you are on-call, and a member of the root mail alias.
- You get to Friday morning, looking forward to completing some OS upgrades, take the afternoon off.
- There are 50 voice-mail messages from people who cannot read their email. Logging onto the machine you find:
 - The mail spool is filled, having doubled in size overnight.
 - The outgoing queue has 10,000 messages in it.
 - Your mailbox is filled with hundreds of complaints, many of them nasty and vicious, accusing you and the school of all manner of low acts for supporting “spammers.”
 - And, you find that many places will not accept mail connections from your school because you are harboring “spammers.”
- Raise your hand if this has this happened to you? If it hasn't, you're lucky.

Overview:

- What is spam?
- How does Spam Spread?
- Promiscuous Relaying
- Server Solutions
- Client Solutions
- Community Solutions
- Conclusion
- Spam Resources

Slide 2

Notes for slide 2:

A quick overview of the rest of this talk

- What is spam? A brief history, some terminology. Spam occurs in many forms, we will be mostly concerned with email spam, or spam-lite.
- How does Spam Spread? Spam needs to get from machine A to machine B, how does it do this.
- Promiscuous Relaying: We will talk a lot about machines which relay mail, when is this good? Why is it usually bad.
- Server Solutions: Server bases solutions to Spam, especially email spam.
- Client Solutions: What can end-users do?
- Community Solutions: What can we do as part of the larger community of system administrators, and as members of the Internet.
- Conclusion
- Spam Resources

What is Spam?

- Spiced Pork And Meat (Hormel)
- Inspiration for Poetry
- Crashing a program via buffer overflow
- Massive cross-posting, or off topic News
- Mass, Unsolicited Commercial Email (UCE)
- Mass, Unsolicited Non-commercial Email
- Mass, Solicited Email
- Chain letters

Slide 3

Notes for slide 3:

What is Spam?

- Originally, it meant Spiced Ham and Meat, and that is the definition that Hormel, the trademark owners of SPAM wish to maintain.
- It is also inspiration for poetry, as seen on the next slide.
- *The Hacker's Dictionary*, 1991 gives as the definition of Spam: [from the MUD community] vt. To crash a program by overrunning a fixed-size buffer with excessively large input data. *The Contradictionary*, 1995 by Stan Kelly-Bootle gives the same definition. So, Spam in the sense we are using it today is, in net terms, fairly recent.
- Over the past couple of years, to computer people, spam has come to mean:
 - Massive cross-posting or repeated posting of, generally, off topic articles to Usenet.
 - Mass, Unsolicited Commercial Email.
 - Mass, Unsolicited Non-commercial Email, such as please to write your representative about a important political issue, or for help in finding a missing person.
 - Mass, solicited Email: That is, a mass mailing to people who signed up for a service.
 - Chain letters.

Spam-Ku

Can of metal, slick
Soft center, so cool, moistening
I yearn for your salt

Silent, former pig
One communal awareness
Myriad pink bricks

Slide 4

And who dares mock Spam?
You? you? you are not worthy
Of one rich pink fleck

Oh tin of pink meat
I ponder what you may be:
Snout or ear or feet?

Old man seeks doctor
"I eat Spam daily", he says.
Angioplasty

Notes for slide 4:

There is actually a book of Spamku, *Spam-Ku: Tranquil Reflections on Luncheon Loaf*, John Cho, editor.

A Brief History of Spam:

- April 12, 1994, Green Card cross-posting
- Jeff Slaton, Route 66, and Atomic Bomb plans.
- Sanford Wallace, and Cyber Promotions.

Slide 5

Notes for slide 5:

- April 12, 1994, Green Card cross-posting:
 - Two lawyers in Arizona, Laurence Canter and Martha Sigel, sent an advertisement to over 6,000 newsgroups. Advertising services with the “Green Card Lottery.”
 - So many complaints were sent to their ISP that the mail server crashed, and they lost their account.
 - Canter and Sigel later wrote a book: *How to make a Fortune on the Information Superhighway*).
 - In the book, they told how to gather email addresses from Usenet, how to send junk mail, post commercials on Usenet, advertise on IRC, etc.
- Jeff Slaton, Route 66, and Atomic Bomb plans:
 - One of the readers of Canter and Sigel was Jeff Slaton, a Yellow Pages representative at US West Direct, in Albuquerque, MN.
 - He gathering email addresses and asked Route 66, his ISP, if they would mind if he sent out a mass advertisement.
 - They said, yes, he would mind, and suggested he read a book about making money on the Internet instead.
 - Well, he had read a book, but it was the wrong book.
 - Two days before his account expired, he sent out an advertisement for the “original plans for the atomic bomb, \$18.00.

- Slaton claims he sold thousands of copies world-wide.
- Slaton went on to be the first to offer spamming as a service, and billed himself as The Spam King. He was also the first to forge a fictitious return address to divert complaints.
- Sanford Wallace, and Cyber Promotions.
 - No brief history would be complete without mentioning Sanford Wallace, and Cyber Promotions.
 - In the spring of 1996 Sanford (later to be know as Spamford) took the Spam king crown for himself.
 - He was also the first to Spam AOL, and AOL and he have exchanged lawsuits. And so have Cyber Promotions and Prodigy, CompuServe, Concentric Networks, etc.
 - Wallace was suing because these ISP's were blocking his advertisements.
 - They were suing because cyber promotions would forge AOL return addresses.
 - The entire history of Cyber Promotions can be found in Schwartz and Garfinkle, Appendix B.
 - If you had an AOL account during the days of Cyber Promotions, you know of the problems Spam caused: people would log in and find 50 or 60 messages a day, all of them spam, which they had to pay to download.

Why Is Spam Bad?

- The economics are wrong:
 - The recipient pays most of the cost.
 - The sender pays too small a cost.
- Hidden Costs
 - Larger servers
 - Admin time.
 - User time deleting
- Degradation of service
- Lack of accountability
- Theft of service and reputation
- The Future: It just doesn't scale

Slide 6

Notes for slide 6:

- Why is SPAM bad? Isn't it just like other advertisements? You will hear many arguments, mostly con, but some pro. Why is spam bad?
 - The biggest problem is, the economics are wrong. They are wrong because:
 - * The recipient pays most of the cost.
 - * The sender pays too small a cost.
 - Absent negative feedback in the for of paying the cost of advertisement, advertisers are encouraged to advertise more.
 - Hidden Costs: Larger servers, admin time put into cleaning up after a spam attack, time to delete spam.
 - Degradation of service: AOL's message system was rendered useless for a time by Cyber Promotions.
 - Lack of accountability—often intentionally. Who is advertising? Can you trust them?
 - Theft of service and reputation, when spam is distributed through third parties, or complaints are redirected to an innocent bystander.
- The Future of Spam: The number one problem, It just doesn't scale. (Read from page 41 of Schwartz and Garfinkel.)

How Does Spam Spread?

- Original Spam: Usenet.
- Canter and Sigal Green Card post:
- Then it got out of hand:
 - Spam Cancels
 - Usenet Death Penalties
 - Good Housekeeping cancel services.

Slide 7

- Cancels chasing Spam.
- Cancel Strike, ISP filters.
- Spam-lite: email
 - Cyber promotions
 - Get Rich Quick
 - Chain-mail,
 - Virus alerts
- Chain mail insignificant compared to UCE.

Notes for slide 7:

How Does Spam Spread: Two basic varieties Usenet and email.

- Original Spam: Usenet.
- Spam started on Usenet with the Canter and Sigal Green Card post. From there it really got out of hand.
 - Spam Cancel Services (e.g, CancelMoose).
 - Usenet Death Penalties.
 - Auto-Cancelers, using the Breidbard Index ($\text{copies} \times \sqrt{\text{newsgroups}}$).
 - Good Housekeeping cancel services.
- This war was going full force when I inherited Usenet.
- At one point it seemed half of Usenet traffic was cancel messages chasing the other half.
- April 3rd, 1998 the cancelers went on strike.
- By the 17th, enough ISP's ran filters to have an effect.
- Spam-lite: The other spam is email, which includes not only the cyber promoters, but also chain-mail spam, get rich quick schemes, urban legends, virus alerts, etc.
- Over time, the chain mail—while still a problem—has become insignificant compared to the UCE relayers.

Promiscuous Relaying:

- SMTP: Simple Mail Transport Protocol
- Purpose of SMTP: Relaying email
- Originally, anybody could relay
- Still the default out-of-box
- Invitation to be exploited by spammer
- Solution: Restrict relaying

Slide 8

Notes for slide 8:

Promiscuous Relaying:

- The Simple Mail Transport Protocol is used to send email around the Internet.
- The most common programs which implement SMTP are sendmail, qmail, smail, Netscape Messenger, Pegasus Mercury Mailer, Post.Office, and others.
- Sendmail, qmail and smail probably handle 90
- The purpose of an SMTP server is to relay mail, so why is relaying bad?
- It isn't: promiscuous relaying—relaying email for just anybody—is bad.
- Once the standard, still the default:
 - Audit lines were in the message for debugging
 - Servers started doing reverse lookups to identify the sending machine.
- Machines configured in this way now are open invitations to be used to relay spam.
- The solution is to restrict relaying.

Server Solutions:

- Block The Sender IP or Account
- Blocking has several disadvantages:
 - Takes place after the fact
 - Blocking a users easy to get around
 - Blocking an IP address blocks everybody
 - Difficult to keep lists up-to-date

Slide 9

- Mail Abuse Prevention Systems: Realtime Black-hole List.
 - Uses a DNS server to distribute IP addresses
 - RPI once on the list
 - Block legitimate mail
 - Other checks as effective
- Sanity Check Sender
- Blocking Promiscuous relaying.

Notes for slide 9:

Server Solutions:

There are a variety of proposed solutions to dealing with Spam.

- Blocking senders.
 - Block the sending sight by name or IP address.
 - Block the spammer by account name.
- Blocking has several disadvantages:
 - Takes place after the fact.
 - Blocking a users is easy to get around.
 - Blocking an IP address blocks everybody
 - Difficult to keep lists up-to-date.
- Mail Abuse Prevention Systems: Realtime Blackhole List.
 - Uses a DNS server to distribute IP addresses of “Spam Friendly” sights.
 - Many ISP’s are using this.
 - RPI is not, but we were once on their list.
 - It would block more legitimate mail than spam.
 - Other checks were just as effective.
- Sanity Checking sender.
 - Spammers frequently use forged return addresses

- Is the return address valid?
- It is also possible to check if the full address is valid using SMTP's `vrfy` command.
- Many ISP's refuse `vrfy` requests.
- sendmail 8.9 can pattern match headers.

Blocking Promiscuous Relaying:

- Most machines relay
- Problem is, relaying for anybody
- Central Server:
 - Mail Originates in domain
 - Mail destined for domain
- Desktop machine: Relay to/from self
- Or, don't run SMTP server
- Limits spammer's ability to spam

Slide 10

Notes for slide 10:

Blocking Promiscuous relaying:

- Most machines that can send or receive mail relay—that's how mail gets delivered.
- The problem is allowing relaying by too many untrusted machines.
- A server usually relays mail within a domain.
- otherwise the mail must originate from the domain, or be destined for an account within the domain.
- The typical desktop machine need not relay to anybody but itself.
- Even that might be too much. Does the machine have to receive mail? Can mail be read from a central server?
- Restricting relaying reduces spam destined to others, and makes it harder for spammers to operate. It is also keeps your domain from appearing in the header of a get rich quick scheme.

Client Solutions

- The Delete Key
- Filters
- Procmail for System-Wide Filtering
- Address Munging
- Email Channels `http://lpwa.com:8000`

Slide 11

Notes for slide 11:

Client Solutions:

- The Delete Key: One of the quickest ways to eliminate spam, but not always practical—low signal to noise ratio makes email less useful.
- Filters: Eudora, Outlook, Netscape, elm, all allow the user to define filters.
- Procmail is a local delivery agent which allows users to define filters. It can also be used to setup system-wide filters.
- Address munging: Don't give out email addresses, or give out only a munged address which a program cannot interpret.
- Robert Hall at AT&T has developed a system of email channels, which can be used to restrict who can send you email (`http://lpwa.com:8000` has a service based on this idea.)

Community Solutions:

- Reporting Spam (accurately)
- Boycotting Companies (explain reasons)
- Anti-spam Legislation (carefully)
- Anti-spam Vigilantes (avoid)

Slide 12

Notes for slide 12:

Community Solutions:

- Reporting Spam: It's easy to just delete it, it takes time to report it, and it takes more time to report it politely and accurately.
- Boycotting Companies: Some people boycott companies that advertise spam. Most of the companies don't care, but some might. Some might not be aware that UCE is a controversial method of advertising.
- Anti-spam legislation: Several bills have been proposed. Some would legitimate spam, others would forbid sending advertisements with a forged return address. Virginia recently passed such a bill.
- Anti-spam vigilantes: Giving away the home telephone number of spammers, sending fax loops, denial of service attack against servers. MAPS? UDS?

Conclusion:

- Relentlessly Disable Relaying
- Police and Educate Users
- Respond to Complaints
- Blame the Right Parties
- Avoid Vigilantes
- MAPS, UDS? Borderline cases

Slide 13

Notes for slide 13:

Conclusion:

- Relentlessly disable promiscuous relaying.
- Police and educate Users.
- Respond to complaints. It isn't easy, but it must be done.
- Blame the right parties—usually not the sender.
- Avoid vigilantes.
- MAPS, UDS? Borderline cases.

Spam Resources:

- *Sendmail*, by Costales, with Allman, ORA, 1997.
- *Stopping Spam*, by Schwartz and Garfinkel, ORA, 1998.
- <http://www.sendmail.org/>, <http://www.sendmail.com/>: Free and commercial sendmail, with links to anti-spam pages.
- <http://www.sendmail.org/~ca/email/check.html>: Claus Aßmann's anti-spam provisions.
- <http://www3.mids.org/mn/704/spam.html>: Article from *MicroTimes*.
- <http://www.cauce.org/>: Coalition Against Unsolicited Commercial Email.
- <http://maps.vix.com/>: Mail Abuse Prevention Systems: Realtime Blackhole List.
- <http://antispam.shmooze.net/spamdrive/>: The AntiSpam Mail List's SPAM Drive.
- <http://www.npr.org/programs/atc/archives>: For you NPR junkies, All Things Considered had two articles about spam, April 17, 1998 and July 14, 1998.

Slide 14