Email Security And Anti-Spam Tutorial

NLANR/Internet2 Joint Techs
Columbus, Ohio July 18, 2004

Joe St Sauver, Ph.D.
University of Oregon Computing Center
joe@uoregon.edu

http://darkwing.uoregon.edu/~joe/jt-email-security/

Introduction

A Little About This Talk

- Paul Love was good enough to invite me to do this tutorial today
- I'm not sure there's much to be said about spam and email security that hasn't already been said, but I'll see if I can't find at least a few new things to share with you this afternoon.
- Some of the information we're going to cover may be "old news" for some of you, and for that, I apologize; folks attending may have radically different levels of expertise.

Sticking To The Script

- Because we have a lot to cover, and because many spam fighting folks from your institutions who may not be attending today, I've prepared this tutorial in some detail and will try to "stick to the script."
- This is a good news/bad news thing: if you're looking at this presentation after the fact, you'll be able to follow what was covered; the bad news is that if you're in the audience today, there won't be a lot of "surprises" mentioned during the tutorial that aren’t in this handout.

Format of Today's Tutorial

- We're going to begin by talking about email security
- We'll take a little break
- After the break we'll talk about anti-spam measures
- At the end we can talk about email security issues or spam issues you may be confronting, either here or over beers later in the bar.

Email Security

Email Security Is Really Just One Facet of Sound Overall System and Network Security

Email Security and Its Role in Your Overall Network Security Plan

- Many of the network security threats you face are directly tied to email security issues.
- Unfortunately, because email is considered to be rather "mundane" or plebian, email security issues sometimes get short shrift.
- In point of fact, email security deserves extra attention because it is the one application that is truly ubiquitous, and is truly mission critical.
- We'll assume you're working in a Unix-based email environment, as is true at most I2 schools.

Mail Encryption

Encrypt Your POP & IMAP Traffic

- Hacker/crackers *love* to sniff wired or wireless ethernet traffic for usernames and passwords.
- One of the most common sources of usernames and passwords on the wire consists of clear text POP and IMAP logins to campus mail servers, particularly when users routinely set their email clients to login and check for new mail every minute or two.
- That sniffed username and password will commonly provides access to confidential email, which is bad enough, but it may also provide access to other campus resources.
- If you are NOT currently requiring encrypted POP and IMAP logins, the time has come to do so.

Encrypt Your POP & IMAP Traffic (2)

- Most popular POP and IMAP clients and servers now support TLS/SSL encryption, including Eudora, Outlook, Entourage, Mozilla, Mulberry, OS X's Mail program, etc.
- See the recipes for enabling TLS/SSL encryption: http://micro.uoregon.edu/security/email/ (we're happy to get submissions of new "recipes" for other TLS enabled mail clients, too!)

SMTP Auth With STARTTLS

- What about SMTP?
- While you're encrypting POP and IMAP traffic, you might as well also require SMTP Auth (RFC 2554) over a TLS encrypted channel. See: www.sendmail.org/~ca/email/auth.html
- If you do deploy password based SMTP Auth, be SURE that you require strong user passwords (check 'em with cracklib). Spammers will try exhaustive password attacks against servers using SMTP Auth in an effort to remotely relay (e.g., see: http://www.winnetmag.com/Articles/Print.cfm?ArticleID=40507). Watch your logs/limit bad password attempts/tarpit abusers!

Controlling Other Plaintext Password Exposures

- If you also offer a web email interface, be sure it is also always encrypted (runs via "https") too.
- Require ssh (not telnet or rlogin) for any access to Pine or similar command line email programs.
- Replace ftp with scp or sftp, etc.
- Work to eliminate any legacy shared (rather than switched) network segments (switched ethernet is not a panacea, true, but it can help)
- SecureID/CryptoCard-type token based auth systems may also be worth testing/evaluation
- We'll come back to passwords later…

A Brief Crypto Diversion: GPG

- Encourage your users to try Gnu Privacy Guard http://www.gnupg.org/
- Public key message encryption is particularly important for your administrative users, who may be moving around files full of social security numbers or other sensitive information
- Are you currently issuing GPG-signed security announcements? Are your users checking those signatures for authenticity?
- What's your key management solution?
- Are you holding key signing parties?

Anti-Virus

Neutralize Viruses and Worms

- Your users face a constant barrage of inbound viruses, worms and other dangerous content. Remember all the viruses "fun" of Fall 2003? [http://www.syllabus.com/news_issue.asp?id=153&IssueDate=9/18/2003 (and 9/25/2003)]
- Depending on your email architecture, you may be able to run each message through an AV scanner such as ClamAV (a GPL-licensed Unix antivirus product, see: http://www.clamav.net/)
- If/when you do find viruses, please do NOT send non-delivery notices to forged message body From: addresses! (see http://www.attrition.org/security/rant/av-spammers.html)

Attachment Defanging/Stripping

- If you can't run a antivirus gateway product on your mail server, you should AT LEAST "defang" all executable attachments by having procmail stick a .txt onto the end of the original filename. [Attachments that are particularly likely to contain dangerous content (such as pifs and scrs) should get stripped outright from incoming messages]. See http://www.impsec.org/email-tools/procmail-security.html for a defanger
- Be sure to spend some time thinking about how you want to handle zip files, passworded zip files with the password included in the body of the message alongside the zip file, .rar files, etc.

Handling The Viruses That Get Detected

- If you do have a program that strips viruses from incoming email, is it smart enough to NOT send misdirected "you've got a virus!!!" warnings to thousands of forged From: addresses every day?
- Bogus virus warnings can be a bigger problem for your users and neighbors than the actual viruses themselves…

Risks of Sending Bogus AV Notifications

- In fact, the problems associated with bogus antivirus notifications have become so severe that some sites have begun to automatically block all email coming from sites that have broken antivirus gateways.
- See, for example the 127.0.0.9 code at http://www.five-ten-sg.com/blackhole.php and http://www.attrition.org/security/rant/av-spammers.html
- Educate your antivirus software vendors!

Users Still Need Desktop Anti Virus Software, Too

- While you will likely do a good job of blocking viruses sent through your central email servers, users do still need a desktop AV product to deal with viruses coming through other email servers, infested web pages, peer to peer applications, instant messaging, Usenet, IRC, CIFS, etc.
- When site licensed, commercial desktop A/V products can be surprisingly affordable.
- Site license an A/V product for ALL members of the University community! Any user's system can be a spewing mess without it!

Some Antivirus Vendors

- UO currently site licenses Norton Antivirus from Symantec, however, there are also other commercial antivirus programs you should evaluate, including…
  http://www.grisoft.com/
  http://www.kaspersky.com/
  http://us.mcafee.com/ (caution: pop up ads!)
  http://www.sophos.com/
  http://www.symantec.com/
  http://www.trendmicro.com/

Some Free Antivirus Products for Home Use

- Avast! 4 Home Edition
  http://www.avast.com/i_kat_76.html
  (free for home use)
- AVG Free Edition
  http://www.grisoft.com/us/us_dwnl_free.php
  (for single home users, cannot be installed on servers, cannot be installed in a networked environment; the do also offer a 30 day free trial download of AVG 7.0)

Create a "Virus Resistant" Email Culture

- A key determinant of the level of problems you have with viruses is your local "email culture"…
  -- Are non-institutional email accounts common?
  -- Do users routinely send plain text email only, or are attachments used even for short notes?
  -- Do users tend to employ a simple command line email program (such as Pine), or a more complex email program that's tightly coupled to the underlying operating system (like Outlook)?
  -- Do users have a sense of healthy skepticism (regarding VISA phishing, 419 scams, etc)?

Email Security and Monoculturality

PCs Running Windows

- Two market share factoids:

  -- PCs running Windows represent ~94% of the desktop market as of late 2003 (see: http://content.techweb.com/wire/story/TWB20031008S0013)

- -- Internet Explorer is the dominant web browser, also with a ~94% market share http://www.nwfusion.com/news/2004/071204browser.html

Considering Alternative Operating Systems…

- A monocultural Microsoft-centeric desktop environment creates certain risks that an environment consisting of a mix of PCs running Windows, Macs and Linux boxes doesn't have.
- Others have already noticed this, and are taking steps to move their organizations away from 100% reliance on Microsoft Windows. For example…

The Non-Windows Desktop

- '"Our chairman has challenged the IT organization, and indeed all of IBM, to move to a Linux based desktop system before the end of 2005," states the memo from IBM CIO Bob Greenberg...' http://www.eweek.com/article2/0,4149,1494398,00.asp
- "Scientists: The Latest Mac Converts" http://www.ecommercetimes.com/perl/story/32837.html
- "Mac OS X Site License Available [at the University of Oregon]" http://cc.uoregon.edu/cnews/winter2004/osx.html
- "Two U.K. government agencies—with more than 1.2 million desktop computers combined—announced in recent months that they would use desktop Linux and other open source software." http://www.reed-electronics.com/eb-mag/index.asp?layout=article&articleid=CA376443&industryid=2117&rid=0&rme=0&cfd=1
- "[Dave Thomas, former chief of computer intrusion investigations at FBI headquarters] told us that many of the computer security folks back at FBI HQ use Macs running OS X, since those machines can do just about anything: run software for Mac, Unix, or Windows, using either a GUI or the command line. And they're secure out of the box. * * * Are you listening, Apple? The FBI wants to buy your stuff." http://securityfocus.com/columnists/215

Changing "Religions" Aside…

- Let's assume you're stuck running Windows, at least for now…. what should you do to be as secure as possible within that overall constraint?
- You know the key concept, but I'm compelled to recite it here for completeness:
  -- upgrade to a currently supported version of the operating system, and be sure you've
  -- applied all service packs and critical updates
- Be sure that future critical updates and service packs also get automatically applied

Note Well: Automatically Applying Patches Is Not Without Its Own Risks

- I've personally had three production W2K servers get blown off the air by a single automatically-applied updates (thankfully all three were subsequently recoverable via SFC /SCANNOW). Trust me when I tell you that automatically patching can be risky.
- I highly recommend you read "Patch and Pray" http://www.csoonline.com/read/080103/patch.html ["It's the dirtiest little secret in the software industry: Patching no longer works. And there's nothing you can do about it. Except maybe patch less. Or possibly patch more."]

Trust, But Verify

- Scan your own networks to make sure your users are patched up to date… Microsoft has tools at http://www.microsoft.com/technet/security/tools/default.mspx
- Commercial scanning products are also available, and may probe more for additional vulnerabilities/issues; nice review of some options at http://www.pcmag.com/article2/0,4149,1400225,00.asp (Dec 30, 2003)

There's More to Basic Windows Security Than Just Getting Critical Updates Done!

- Once you've gotten your system up-to-date in terms of critical updates, you are not done; there are many additional important things you should do to harden your Windows system.
- A brief list of the top vulnerabilities to check and correct is at http://www.sans.org/top20/
- For a detailed study, see: *Microsoft Windows Security Inside Out for Windows XP and Windows 2000*, Microsoft Press (800 pages).
- **http://www.columbia.edu/kermit/safe.html**

Spyware

Spyware

- At the same time you deal with desktop antivirus requirements, be sure you also handle spyware. Spyware includes things such as web browser hijacking programs, key stroke loggers, long distance dialer programs, etc. You might think that antivirus programs would also handle these type of threats, but they usually don't.
- "Experts suggest that [spyware] may infect up to 90 percent of all Internet-connected computers." http://www.technewsworld.com/story/security/33465.html (April 16, 2004)

Coping With Spyware

- A variety of anti-spyware packages were recently reviewed by PC Magazine; see: http://www.pcmag.com/article2/0,1759,1523357,00.asp (2 Mar 2004)
- One particularly popular anti-spyware program at UO is Spybot Search & Destroy from www.safer-networking.org/en/index.html

Some Anti-Spyware Tips

- Coverage across products won't be perfect; use multiple products to cover the "corner cases" any single anti-spyware product may miss.
- To help avoid getting spyware, avoid P2P applications, instant messaging applications and the files shared via those channels.
- If all you're seeing are ads popping up on your display, be sure Messenger is disabled; see: http://www.stopmessengerspam.com/

Firewalls

Software and Hardware Firewalls

- Some of you may have a hardware firewall installed at the border of your network. That's fine, but it's no longer where it needs to be – the way some recent worms have ripped through large networks have made that clear. See, for example, "Picking At a Virus-Ridden Corpse: Lessons from a Post-Blaster, Post-Welchia, Post-Nachi, Post Mortem," http://www.syllabus.com/news_issue.asp?id=153&IssueDate=9/18/2003

Desktop Firewalls Are Needed

- You should be looking at per-workstation software firewall products (or inexpensive personal hardware firewalls, such as those from Linksys), instead of (or in addition to) your border firewall, much as you currently deploy anti-virus software on each desktop.
- This is routine practice on residential broadband networks; the rest of us need to catch up.

One Bit of Good News…

- The next major update for Microsoft Windows XP will have Microsoft's integrated Windows Internet Connection Firewall (ICF) "on" by default. This will make a huge difference for your Windows XP users (assuming they install that update!), however don't lose sight of the fact that most sites typically have systems running many earlier versions of Microsoft Windows (which lack the ICF).

Some Notes About Software Firewalls

- Note that many "free" software firewalls aren't actually licensed for free institutional use!
- If using a software firewall, beware of ongoing maintenance costs.
- Novice users can also easily be confused when it comes to making decisions for software firewalls about what applications to accept or block.
- One review of personal software firewalls: http://grc.com/lt/scoreboard.htm

Personal Hardware Firewall Thoughts

- Hardware firewalls can be installed "backwards," in which case they can act as a rogue DHCP server, handing out RFC1918 addresses to everyone on their subnet.
- Some hardware firewalls may use uPnP if not carefully configured: http://cc.uoregon.edu/cnews/spring2003/upnp.html
- Some hardware firewalls may come bundled with wireless access points (which have their own security issues)
- Reviews? See: http://grc.com/lt/hardware.htm

An Unexpected Consequence of Deploying Desktop Firewalls

- There is one unexpected consequence of deploying desktop firewalls that you should be aware of: once users deploy a desktop firewall, particularly if they deploy a software firewall product, they will be amazed by just how often their systems are getting probed. The level of ongoing "background radiation" associated with hacker/crackers activity can be fairly shocking to folks who aren't routinely doing security-related work.

Another Unexpected Consequence of Deploying Personal Firewalls

- You and your staff will lose the ability to scan your own users for vulnerabilities (but that's going to happen anyway with SP2)
- Have you thought about what you plan to do once your end users' workstations become opaque?

Passwords

Passwords

- Once users know how often hacker/crackers are “poking” at their systems, the importance of strong system access controls becomes much more understandable, although most universities still rely on usernames and passwords rather than hardware crypto tokens or other advanced authentication solutions, largely because of the cost of those alternatives ($60 to $70 per token or more).

Of Course, Regular Passwords Aren't Really "Free"

- Gartner estimates that up to 30% of calls to a typical helpdesk are password related. (http://www.nwc.com/1317/1317f13.html)
- Estimates for the cost/call vary widely, but let's hypotheticall assume you use comparatively inexpensive interns, and peg that cost at $5/call (it is probably far higher when you think about the lost productivity of the employee with the password problem). How often do YOUR users forget/need to have their passwords reset?

It might make sense to look at more secure alternatives…

- When you factor in the actual costs of using "free" passwords, and the improved security that hardware tokens or other advanced methods can offer, it might make sense to begin moving away from plain passwords. A nice discussion of some of the issues is available at http://www.giac.org/practical/GSEC/Lawrence_Thompson_GSEC.pdf

If You're Stuck With Passwords

- Do you insist that your users choose a strong password? (If at least some users aren't complaining, those passwords probably aren't as crack resistant as they should be)
- Do they require users to periodically change their password? How often?
- How do passwords get assigned and distributed? How do they get reset if forgotten?

Email Security Pot Pouri

Some Random Thoughts

- Do all messages, whether internal or external in origin, go to the same mail exchangers? Might there be some value in sending external email to different MX's than internal mail?
- Is email always getting delivered to your most prefered MX, or are spammers sending mail via less preferred MX's that might have lower quality spam shielding than your main MX's?

Some More Random Thoughts

- What's the I/O load on your mail spool look like? Are you getting close to saturation? What's your plan for accommodating any incremental load, such as load associated with larger quotas as schools play "let's keep up with Gmail?" (see: 'Welcome to Your Weekly Paradigm Shift: Large "Free" Web Email,' http://www.syllabus.com/news_article.asp?id=9745&typeid=153)
- What file system are you using? Something UFS-related? Or something more modern, like Reiserfs?

Quick Break

- Before we go into the anti-spam section of this talk let's take a five minute break

Anti-Spam

Our Goal:
Email "the Way It Used to Be"

- Our goal: **Email, the way it used to be.**
  That implies that spam will be virtually non-existent, and that normal academic communication can take place with minimal games -- no need to conceal your address from most of the world, no worries about posting to mailing lists w/o munging your address, no challenge-response BS, etc…

The UO End User Email Experience

- We generally meet that goal: our users see little if any spam on our large central systems. Most users see none (zero spam per day). Some users will occasionally see "whack-a-mole" spam pop up from a reputable provider who briefly has a bad customer.
- True anecdote: every once in a while we get complaints about spam getting "bad:"
  "Hey, what is going on over there!
  I got three spam in my mail this last week!!!"

Your University Can Achieve The Same Level of Spam Filtering Efficiency

- There's nothing magic about what we're doing.
- We're going to explain what we believe is happening, and how you can deal with it as we have.

But First, Let's Begin With Some Spam Statistics For Context

Ferris Research Spam Report

- "Cost of Junk Email to Exceed **$10 Billion** for American Corporations in 2003" http://www.ferris.com/pub/FR-126.html

Ferris Research Spam Report (2)

- For comparison:
  -- Federal funding for global AIDS, tuberculosis and malaria programs: **$2.2 billion** (www.medicalnewstoday.com/medicalnews.php?newsid=9923) (25 June 2004)

  -- NSF budget request for FY2005: **$5.745 billion** http://www.nsf.gov/bfa/bud/fy2005/pdf/fy2005_1.pdf

  -- OR personal income tax revenues for the 2003-2005: **$9.9 billion** (http://www.oregon.gov/DAS/BAM/docs/Publications/GBB0305/Q-RevenueSummary.pdf)

  -- Cost of the war in Iraq and Afghanistan: **$60 billion** http://www.usatoday.com/news/washington/2004-06-27-war-costs_x.htm

The Nucleus Research Spam Report

- "Nucleus conducted in-depth interviews with employees at 82 different Fortune 500 companies - the same companies interviewed a year ago. Some of the key findings in the report include the following:
  "-- **The average employee receives nearly 7,500 spam** messages per year [e.g., 20.5/day], up from 3,500 in 2003.
  "-- Average lost productivity per year per employee is 3.1 percent [e.g., 15 minutes/day], up from 1.4 percent in 2003.
  "-- Companies using spam filters report that **on average they are able to filter only 20 percent of the incoming spam**, down from a reported 26 percent in 2003."
  "…**the average cost of spam per year per employee more than doubled from the previous year to $1,934**"

  www.nucleusresearch.com/press_releases/prspam2.html

2 Trillion+ Spam/Year Sent to U.S. Users

- "Email pests on the rise: **2 trillion spams in US alone**" (http://www.nbr.co.nz/home/column_article.asp?id=7965&cid=3&cname=Technology)

  [Assumes each user receives 20 spam/day, 365 days/year, with 182 million US Internet users (http://ecommerce.insightin.com/player/internet_user.html) and assuming 2 spam sent=1 spam received. That implies 2.65T spam were sent to US users last year.]

Some Industry Spam %-age Estimates

- “Spam remained steady at 78% during May 2004.” (http://www.postini.com/press/pr/pr060704.html)

- ‘A report released last month by MessageLabs, Inc., an email management and security company based in New York, showed that nine out of 10 emails in the U.S. are now spam. Globally, 76 percent of all emails are spam. And Osterman [founder and president of Osterman Research] says the problem is only going to get worse. "In the next year to a year and a half, spam will account for 98 percent of all email," he says. "That's being pessimistic some would say. The optimistic forecast is that it will only get to 95 percent.”’ (July 1st, 2004) (http://www.internetnews.com/stats/article.php/3376331)

Pew Internet and American Life Project: "Spam – How It Is Hurting Email and Degrading Life on the Internet"

- 73% of email users avoid giving out their email address
- 69% avoid posting their email address on the web
- 70% of email users say spam has made being online unpleasant or annoying (http://www.pewinternet.org/pdfs/PIP_Spam_Report.pdf) (Oct 22, 2003)

Filtering vs. Not Filtering

Despite those statistics, there ARE American universities that don't do spam filtering….

http://darkwing.uoregon.edu/~joe/jt-email-security/university-spam-strategy.xls

So What *If* We Just Did Nothing?

- Doing nothing is fraught with potential problems…

  -- Spam has the potential to act as a denial of service attack against "real" mail.

  A) Real messages may easily get missed in amongst all the spam.

  B) Accounts may go over quota from spam, and begin bouncing all email.

  C) Spam sent to mailing lists you host may get sent on to subscribers, who may then unsubscribe from those lists.

Doing Nothing (2)

- -- If you choose to do nothing about spam, there will be a tremendous amount of wasted staff time as staff deal with the spam which they've been sent (plus the temptation to waste still more work time on non-work-related "content" being advertised in the spam they receive).

  What's a half hour or hour a day per employee worth to your school?

Doing Nothing (3)

- -- If you do nothing about spam, users will create email accounts on 3rd party services which offer ***some*** sort of filtering. Do you really want institutional business being done from Hotmail? Nah. Others will select and install their own spam filtering solution (good, bad or indifferent) without consulting you or anyone else.

  Doing nothing ==> email chaos reigns.

Doing Nothing (4)

- -- Keeping in mind that much spam may contain particularly objectionable sexually related content, allowing spammers unfettered access to your faculty and staff increases the chance that you may be the subject of a hostile workplace sexual harassment suit. [see: http://news.com.com/2100-1032-995658.html -- I swear I don't make this stuff up!]

Doing Nothing (5)

- If everyone else EXCEPT you filters, you are going to see a tremendous amount of spam as spammers give up on the guys who filter, and devote their attentions solely to the guys who are left.

TANSTAAFL

- The conclusion that you should take action against spam may be pretty much a matter of common sense at this point, but the decision to do so won't be without pain. (There Ain't No Such Thing As A Free Lunch).

  Understanding the implications of deciding to fight spam will be important.

Liability Issues?

- Are there liability issues if we don't deliver all email?
- Technical users of email used to understand that email delivery was NOT assured, and that sometimes email would NOT get through. If it did, great, if it didn't, you'd pick up the phone... Now-a-days, though, many email users seem to assume that email is an assured delivery service (even though it isn't) because it will usually get through…

Blocking Spam == *Censorship?*

- While trying to block spam in good faith, you may be accused of censorship or interfering with academic freedom.
- Some approaches that may diffuse this sort of potentially explosive issue include:
  -- writing your AUP carefully to cover this
  -- allowing individual users to "opt out" from all filtering if they desire to do so
  -- delivering all email, but delivering what's believed to be spam to a different folder than presumptive non-spam email

The "Collateral Damage" or "False Positive" Problem

- The most fundamental cost of blocking spam is the potential for misclassification and rejection of real, non-spam messages by anti-spam measures.
- This is normally called "collateral damage" or the "false positive" problem, and is one of the true (and unavoidable) costs of blocking spam.

When classifying mail, 4 things can happen (2 of which are bad):

- **Actual Case** ***You Believed*** **The Message Was**

  -- Spam Not Spam [oops! **spam got by**]
  Spam [correct classification]

  -- Not Spam Not Spam [correct classification]
  Spam [oops! **false positive**]

- We can get fewer false positives if we're more willing to let more spam slip through, OR less spam if we can accept more false positives. We can't minimize both objectives simultaneously.

So What Should Be Done?

- Finesse the problem. :-)
- Your best bet is probably going to be to spam filter ALL accounts by default, but allow some accounts to "opt out" and be exempt from institutionally- performed filtering on request.

Talk To Your Legal and Senior Administrative Folks

- One procedural note: whatever you decide to do about spam, be sure to talk to your university's attorneys and your senior administration folks before you implement any spam filtering strategy. Spam tends to be highly newsworthy, and there's a distinct chance you'll have a "Chronicle of Higher Education" moment if things go awry. Do NOT surprise your staff attorneys or your Chancellor/President/Provost.

Content-Based vs. Non-Content-Based Filtering

Coping With Spam

- There are many different ways to try to manage spam, but the two most popular mainstream approaches are: (1) to scan messages (including the message's contents) using a tool such as SpamAssassin, or (2) to block messages coming from insecure hosts and known spam sources via DNS-based blacklists (possibly augmented by local filters)
- Other approaches (whitelisting, challenge/ response, hashcash, rate limits, collaborative fitlering, reputation systems, etc.) all have fundamental issues that limit their applicability.

SpamAssassin

SpamAssassin

- By applying a variety of scoring rules (see http://www.spamassassin.org/tests.html) to each incoming message, SpamAssassin determines the likelihood that each message is spam. Typically, messages that look spammy get tagged or filed in a spam folder, while messages that look non-spammy get delivered to the user's inbox.
- While SpamAssassin (or any content based filter) is not our default solution, and not necessarily a solution that we'd recommend, we'll be the first to admit that content based filtering does have some good points.

One Obvious Point In Favor Of Content Based Filtering...

- One obvious point in favor of CBF is that there *is* some spam which is relatively constant, is readily detectable, and is trivially filterable based on its content.
- If you DON'T do CBF and easily identified spam ends up getting delivered, folks will ask, "How come the computer can't ID obvious spam messages when **I** can easily do so?" This is a (sort of) legitimate complaint.

Another Advantage Of CBF

- A second advantage of doing content based filtering is that it allows you to selectively accept some content from a given traffic source, while rejecting other content from that same source. This can be useful if you're dealing with a large provider (such as a mailing list hosting company) that has both legitimate and spammy customers, and you want to dump the spam but accept the legitimate traffic. (But wouldn’t it be better if the large provider kicked off their spammers?)

CBF Issues: False Positives

- On the other hand, one of the biggest issue with CBF is the problem of false positives. Because CBF uses a series of rubrics, or "rules of thumb," it is possible for those rubrics to be falsely triggered by content that "looks like" spam to the filtering rules but which actually isn't spam. For example, some (relatively crude) content based filters make it impossible for a correspondent to include certain keywords in a legitimate email message.

Using Scoring to Minimize False Positives

- Most content-based-filtering software, however, does "scoring" rather than just using a single criteria to identify spam. For example, a message in ALL CAPS might gets 0.5 points; if it also mentions millions of dollars and Nigeria, it might gets another 1.2 points; etc. Messages with a total score that exceeds a specified threshold get tagged as spam; the mere presence of a single bad keyword alone typically wouldn't be enough.

Picking a Spam Threshold

- A CBF issue that's commonly ignored by non-technical folks is choice of threshold value for spam scoring. The threshold value you pick will have a dramatic effect on the number of false positives you see, as well as the number of unfiltered spam you see.
- If you use SpamAssassin, what's your default threshold? 3? 5? 8? 20?
- Do you know the scoring rules you're using, and the weights those rules carry?

CBF and Scaling Properties

- As normally used, sites running Spam Assassin accept all mail addressed to their users, merely running the messages through SpamAssassin to score and tag them, perhaps (at most) selectively filing messages into a "likely spam" folder based on that scoring. Because of this, even if spam does get eventually discarded, you still need to install servers and networks able to initially absorb and temporarily store a virtually unbounded flow of spam. That doesn't scale well.

CBF And The Need To Use All Rules On Each Message

- Doing Content Based Spam Filtering with scoring (ala SpamAssassin) requires that each message be tested against ALL potential filtering tests before acceptance.
- Because CBF applies <n> unique rules to the body of each message that's received, as the number of filtering rules increases, or the size of the message body increases, or both, processing tends to slow down.

Indiana University's Specific Case…

- "When Indiana University installed its new e-mail system in 2000, it spent $1.2 million on a network of nine computers to process mail for 115,000 students, faculty members and researchers at its main campus here and at satellite facilities throughout the state. It had expected the system to last at least through 2004, but the volume of mail is growing so fast, the university will need to buy more computers this year [2003] instead, at a cost of $300,000.
  "**Why? Mainly, the rising volume of spam, which accounts for nearly 45 percent of the three million e-mail messages the university receives each day**."

  "The High, Really High or Incredibly High Cost of Spam"
  Saul Hansell, NY Times, July 29, 2003
  http://www.lexisone.com/balancing/articles/n080003d.html

CBF Issues: The Arms Race

- Because CBF attempts to exploit anomalous patterns present in the body of spam messages, there's a continuous "arms race" between those looking for patterns, and those attempting to avoid filtering. (And remember, spammers can trivially "test drive" contemplated messages through their own copy of SpamAssassin to spot any problems that may block delivery)
- This process of chasing spam patterns and maintaining odd anti-spam heuristic rulesets is rather ad hoc and not particularly elegant.

Spammers Can Simply Out-and-Out Beat SpamAssassin

- I have no desire to provide a cookbook which will help spammers beat filters, so I won't elaborate on this point except to mention one trivially obvious example: because Spam Assassin processing slows down as message size increases, SpamAssassin is generally configured to avoid scanning messages larger than a specific (locally configurable) size. If spammers send messages larger than that size, the spam will blow right past SA…

CBF And Privacy

- Doing content based filtering also implicitly seems "more intrusive" to users than doing non-CBF.
- Even when CBF is done in a fully automated way, users may still be "creeped out" at the thought that their email is being "scanned" for keywords/spam patterns, etc.
- "Big Brother" is a powerful totem, whose invocation should be avoided at all costs.

Non-Content Based Filtering and DNSBLs

It's Not What's In The Message,
It’s Where The Message Comes From That Matters

Holding Sites Accountable

- In the "old days," the Internet worked because most people on the net weren't jerks. If a local jerk did pop up, they were educated or kicked off. You took care of yours; other folks took care of theirs. **Your site valued its reputation**.
- **Times changed**. RBOCs got involved in offering Internet service. Large ISPs came online overseas. Struggling backbones took whatever customers they could get. Malware began to compromise 100s of 1000s of hosts. **The neighborhood went to hell**.

Some of the RBOCs…

- … gave us the "phone company's Internet:"
  -- "'Only" 5% of our users have security issues.'
  -- "We're a common carrier, we're not responsible for what users do on the Internet connections we provide. We'll cooperate with law enforcement if laws were broken and you have a warrant."
  -- Decisions are made based on the business case: "Dealing with abusers is expensive (and reduces our revenues); why bother?"
  -- "We're the phone company, and we don't care because we don't have to care. What are you going to do, FILTER us or something?"

The Internet in Some Overseas Locales

- -- Person-to-person interaction with overseas ISPs is limited, so reputation was/is irrelevant.
  -- Connectivity was/is expensive and had to be paid for somehow.
  -- Some countries had strong privacy protections (which limited provider self-policing options)
  -- Corruption was/is endemic in some areas
  -- Language issues/piracy problems limited access to documentation and vendor support
  -- In some countries "Yankees" are "fair game"
  -- The 3rd world has ITS own phone companies.

<u>Some</u> Struggling Major US Carriers

- While the RBOCs and overseas folks were part of the spam picture/problem, another factor that popped up was that there were some financially struggling major US carriers, who rationalized, "To heck with it. We're struggling, and if we don't sell to Spammer Foo, someone else will. As long as the customer isn't doing something *illegal,* well, why shouldn't I host their web site, do their DNS, etc., etc., etc. They're not actually SPAMMING from here…"

And That's Because of Spam Zombies

- At least 80% of current spam is sent via spam zombies -- end user hosts (usually connected by cable modem or DSL) which have been compromised by viruses or other malware and turned into spam delivery appliances without the knowledge or permission of the system owner. (see: http://www.cnn.com/2004/TECH/ptech/02/17/spam.zombies.ap/ and http://www.sandvine.com/solutions/pdfs/spam_trojan_trend_analysis.pdf)

ASNs With 1% or More of 3.6 Million Open Proxies/Spam Zombies (7/16/04)

ASN	AS Owner	Proxies	%
4134	Chinanet	201160	5.52
7132	SBC Internet Services	166515	4.57
4766	KIX Korea Internet Exchange	132058	3.62
1668	GNN Hosting Service/AOL-Primehost	129851	3.56
7738	Telecomunicacoes da Bahia S.A.	124596	3.42
3320	Deutsche Telekom AG	114188	3.13
9318	HANARO Telecom	107177	2.94
8151	UniNet S.A. de C.V.	98992	2.72
3215	France Telecom Transpac	78771	2.16
27699	TELECOMUNICACOES DE SAO PAULO	71953	1.97
4812	Chinanet/Shanghai Telecom Comp	71637	1.97
8167	TELESC - Telecomunicacoes de S	71141	1.95
4837	CNCGROUP China Telecom China	65506	1.80
3462	HINET Chunghwa Telecom Co.	52173	1.43
9277	THRUNET	51826	1.42
4813	China Telecom/Guangdong China	43002	1.18

Learning More About Open Proxies

- Open proxies are a fascinating topic in their own right, and one you really should learn more about; see my presentation on them at the Kansas Joint Techs last summer: http://darkwing.uoregon.edu/~joe/jt-proxies/

Sidebar: UO's Open Proxy Database

- While traditionally we've made information about open proxies available via a static web page, as the number of open proxies has grown into the millions, that hasn't scaled well.
- As a result, we've now deployed a Postgresql based server, instead at: https://whizzo.uoregon.edu:8443/spamtrack/
- If you want to try it, you'll need a username and password; see me for one at the end of this tutorial, or send me email. [Note: access is discretionary and may be stopped at any time]

What Does This Operationally Mean?

- Blocking spam from known spam sources plus spam from spam zombies/open proxies is easy to do using a combination of DNS blacklists plus local filter rules.

Blacklists

- **Like UO, your university can successfully block the *vast majority* of spam at connection time simply by using a few free (or cheap) DNS blacklists.**
- At the U of O, we use:
  -- the www.spamhaus.org SBL+XBL
  -- the www.mail-abuse.com RBL+ blacklist,
  -- and the njabl.org NJABL DNSBL.
- If you use DNSBLs as we do, endeavor to run copies of those DNSBL zones locally.

Blocking Major Spam Gangs

- The most convenient and elegant way to block most major spam gangs who are sending spam directly to you is through use of the SBL (Spamhaus Block List) from http://www.spamhaus.org/sbl/

  The SBL is free and can be used with sendmail or most other major mail transfer agents. Zone transfers can be arranged for large sites making 400K+ queries/day.

The SBL is NOT Spews

- A more aggressive/controversial approach to blocking known spam sources (which I don't recommend for most colleges and universities) would be to use Spews. Spews is not related to the SBL. Spews attempts to persuade spam-tolerant ISPs to be responsible by using progressively wider blacklist entries.
- For info on Spews, please see: http://www.spews.org/

The mail-abuse.com RBL+

- While the SBL is very good at covering what it says it will cover, it doesn't attempt to cover all the various spam channels spammers try to use. Thus, to block direct-from-dialup spam, spam sent via open SMTP relays, spam sent from some open proxies, and some additional particularly egregious spam tolerant sites, you'll want to use the mail-abuse.org RBL+ See: http://www.mail-abuse.com/rbl+/

The RBL+ Isn't Free (But It Is Cheap for .edu's)

- Not-for-profit and educational sites can license use of the RBL+ in zone transfer mode for $125/name server/year plus $5/thousand users. This translates to about $250/year for a university the size of the University of Oregon. Query mode is also available, but priced so as to discourage its use by large sites. The costs for query access is $150/name server (including 1000 users), with additional users $75 per 500.

The Particular Problem Of Open Proxy Servers

- While the RBL+ recently began to list open proxy servers, the open proxy problem is widespread enough (4 million known open proxy servers at this time), and so popular with spammers that it merits its own supplemental open proxy DNS blacklist. There are a number of open proxy DNSBL's available, but after considering everything, I'd recommend that you use the NJABL (http://njabl.org) open proxy DNSBL.

A Key DNSBL: The CBL (or XBL)

- One key DNSBL that some folks may not be aware of is the CBL (also known as the XBL when accessed via Spamhaus.org)
- You will find the CBL/XBL uncannily effective at blocking open proxies/spam zombies.
- If you run no other DNSBL, I would strongly encourage you to try the Spamhaus.org SBL+XBL combination list (see http://www.spamhaus.org/xbl/index.lasso for more information)

Speaking of Picking DNSBLs

- When you pick a DNSBL, you are effectively trusting someone else's recommendations about what you should block. Not all DNSBLs are equally trustworthy (or efficacious). Research any DNSBL you consider before trusting it with institutional email filtering decisions.
- The three DNSBLs we currently use and recommend all have excellent reputations; they are conservative, accurate and effective.

Are There DNSBLs You Shouldn't Use?

- There are DNSBLs that filter based on anything and everything; I would NOT encourage you to use every DNSBL that someone happens to offer. You really should carefully investigate the criteria used in putting hosts on and taking hosts off the DNSBL (among other things) since you're delegating a tremendous amount of authority to the operators of the DNSBLs you decide to use.

What About Local Filters?

- We'll talk about building local filters later, after we talk about having users report the spam that's still slipping through…

Miscellaneous Filters

- In addition to using DNSBLs (augmented by local filters), we also use some miscellaneous filters such as:
  -- virus filters (covered earlier)
  -- anti-SMTP-relay filters (which everyone uses these days)
  -- some SMTP Mail From: validation checks
  -- a few other miscellaneous rules
- The key components are the DNSBLs plus local filter rules.

DNSBLs Plus Local Filters Work Really Well

- Blocking takes place while the remote mail server is still attached; this means that we can reject unwanted SMTP connections and immediately return the reason to the connecting MTA; no problems with spoofing.
- Spammer content tweaking become irrelevant
- Blocking a single bad connection can translate to avoiding 10K+ pieces of spam; that sort of filtering scales extraordinarily well.

Blocked SMTP Connection Attempts Per Day For Selected Days on Two UO Systems

Date	Gladstone	Darkwing	Total
Sun 14 Jul 2002:	7,405	1,606	9,011
Mon 14 Oct 2002:	16,794	3,452	20,246
Wed 14 Jan 2003:	18,562	5,813	24,375
Mon 14 Apr 2003:	18,714	4,925	23,639
Mon 14 Jul 2003:	15,998	5,116	21,114
Tue 14 Oct 2003:	119,393	9,786	129,179
Thu 15 Jan 2004:	33,289	13,479	46,768
Wed 14 Apr 2004:	59,845	28,339	88,184
Sat 15 May 2004:	59,376	25,401	84,777
Mon 14 Jun 2004:	45,005	49,998	95,003
Thu 15 Jul 2004:	42,612	22,799	65,411

Note #1: Gladstone is our student server, with 27K accounts; Darkwing is our faculty/staff server with 13.5K accounts

Note #2: These are blocked SMTP CONNECTIONS, not blocked MESSAGES. A single SMTP connection may represent 1, 10, 100 or 1000 (or more) MESSAGES.

Note #3: Blocked connections may include viral traffic as well as spam.

User Spam Reporting

When Spam Does Slip Through…

- When spam does slip through our default local filters, we ask UO faculty, students and staff to send us a copy so we can report it to the responsible provider (we like http://www.spamcop.net for this). We also use those reports to tweak our local filters.
- We routinely report spamvertised domains with bad whois data to wdprs.internic.net – those domains then get fixed or disabled.
- It is key that users provide us with timely and usable reports…

Our User Spam Reporting Expectations

- Our goal is to get users to the point where they can consistently:
  -- report only spam they receive (not viruses, not legitimate message traffic), which was
  -- sent directly to one of our spam-filtered systems (not sent through some off site mailing list, departmental hosts, Hotmail, etc.),
  -- to the right local reporting address, within
  -- a day or so of the time the spam was sent,
  -- forwarded with **full/expanded headers** (and with the rest of the message body there, too).

Just Tell Us About Your Spam, Ma'am, Not Viruses

- Users sometimes have a hard time telling spam apart from virus infested messages, and may try to report both. We're really only interested in having spam reported, because (a) viruses aren't intentional, (b) we already "defang" any executable content sent via email, (c) we site license Norton Antivirus for the desktop, and (d) when we complain to ISPs about viruses, those reports seem to accomplish little or nothing.

Teaching Users To Spot Defanged Viruses

- If you defang executable attachments as we do, those executable attachments will all have a three part file name ending in .txt If you can get users to look at the file name of their attachments, you're 99% of the way there.
- Zen paradox: if users shouldn’t open suspicious messages, how do they learn the attachment name?

The Problem Of Users Reporting Legitimate Traffic

- Occasionally users will forget that they have requested email from a vendor about a particular product, or a legitimate email may have a suspicious subject line and may get reported by users wary of opening it. That sort of email obviously isn't spam, and shouldn't be reported, and for the most part doesn't tend to be, although you must be careful when rare cases do arise.

Spam Arriving Via Offsite Mailing Lists

- Occasionally users see spam that came in via some mailing list they're on that's hosted elsewhere. Assuming you use the approach outlined in this talk, spam needs to get filtered by the site that first receives the spam; once the spam has hit a mailing list, it's too late for us to do anything about it. Users need to get the site that's hosting the list to fix their filtering, convince the list owner to make her list closed/moderated, quit the list, live with the spam, or do content based filtering.

We're Sorry You're Getting Spammed on Hotmail, But...

- If your users are like ours, many of them have accounts on Yahoo or Hotmail or other 3rd party web email systems that they use in addition to their institutional accounts. That's fine, but there's nothing we can do to help with spam they get on those accounts, so please don't send it in to us. Likewise, if users are on a departmentally administered host, that's great, but again, there's nothing we can do to fix spam problems there.

Using The Right Local Reporting Address

- While you may be tempted to have local users just report spam they receive to postmaster@<domain> or abuse@<domain> you really should consider creating a special spam reporting address (we'd suggest spam@<domain>) so that spam processing can be kept separate from other postmaster or abuse-related duties. (You should also avoid having users report their spam to your own personal email address.)

Getting Your Spam To Us While It Is Still Fresh

- Users need to understand that spam needs to be reported with a day or so of the time it was sent. Partially this is a matter of dealing with current issues (rather than ancient history that's already been dealt with), and partially this is a practical issue associated with some reporting services such as Spamcop (which needs you to send reports within 72 hours). Three day weekends and vacations are the biggest problem here...

Forward The Spam, Don't Use "Bounce"

- Make sure your users know to use the forward command to send you spam they receive, rather than "bouncing" it to you.
- Why? Forward preserves the integrity of the Received: headers, while bounce tends to comingle the original headers with the headers of the person bouncing the message to you, making it hard to process and report that spam appropriately.

And Then We Come To The Issue Of Full Headers...

- Anyone who works on abuse handling/spam management will tell you that the biggest obstacle to users effectively reporting their spam is getting them to enable full headers.
- My colleagues have built a nice set of how-to-enable full header pages for the email clients that our users tend to use; you're welcome to use them as the basis for local how-to-enable full header pages, too. See http://micro.uoregon.edu/fullheaders/

Providing Full Headers Is Tedious From Some Programs

- If you look through those how-to-get-full-header web pages, you'll see that getting full headers from some email products (such as MS Outlook/Outlook Express) can be very tedious, while in other cases it is a matter of pushing one button. If the email program you or your users use makes it hard to report full headers, complain to that vendor so that enabling full headers can be handled cleanly in future releases of that product.

Yes, You Really Do Want Your Users To Send You Their Spam

- Some of you who may already be drowning in your own personal spam may consider the idea that you want your users to send you their spam, too, to be, well, absurd. Trust me, it's not an insane idea. You NEED your users participation and cooperation because your spam may not look like THEIR spam, and besides, the sooner spam gets reported, the sooner it can get dealt with. Before long, volume will become low.

What Do I Do With Spam After Users Send It In To Me?

- You may want to use http://www.spamcop.net/ to report the spam to the correct providers.
- If you subscribe to the RBL+, be sure to also report any as-of-yet unlisted open proxies or open relays you discover to them.
- You may want to tweak local filters
- You also can report illegal activities directly to appropriate authorities.

Tweaking Local Filters

Locally Maintained Filters As An Adjunct to Blacklists

- Local filter rules let you catch what DNSBLs may miss. We're relatively, uh, "enthusiastic," augmenting the three DNSBLs we use with almost 5,200 locally maintained domain- or CIDR- netblock-oriented rules. If you use sendmail as we do, you'll implement these local filters via /etc/mail/access
- Be sure to use sendmail's delay_checks option
- cidrexpand is your friend
- Think about RCS or other version control

Building Local Filter Rules

- Once you've filtered out the majority of the spam that's being thrown at you, you will find it amazingly easy to deal with the spam that may be left over.
- The basic principle…

Trust Responsible Sites

- Today there are **still** sites, in fact **MOST** sites, which work very hard to deal with security issues (and that includes most of higher education).
- Responsible sites take compromised hosts offline as soon as they're detected. They accept and investigate abuse reports. They refuse to allow spammers to use their facilities.
- Mail from those sites will seldom be a problem.
- They're "good neighbors." Accept mail from them. If something goes wrong and you see spam from them, let them know. They'll take care of it.

Shun Irresponsible Sites

- On the other hand, irresponsible sites ignore abuse reports (or are overwhelmed by the volume of abuse reports they see), and network abuse incidents never gets resolved.
- These sites could address their problems, just as the responsible sites do, but **they choose not to do so**. They're relying on others tolerating their abuse.
- You'll get lots of spam from those sort of sites.
- They're "bad neighbors," and they'll ruin mail for your users, if you let them. Decline to accept mail from them until they take care of their problems.

Why Don't Those Vulnerable Hosts Get Fixed?

- Imagine that you are in charge of a large ISP's abuse desk. (You poor person!) Every morning when you come to work, there are thousands of new complaints about customers with problems -- insecure hosts that have been compromised by hackers, virus infested systems, open relays, open proxies, you name it. No matter how hard you work, more keep coming, day after day.
  You try to prioritize but you never catch up.

Why Don't Those Vulnerable Hosts Get Fixed? (2)

- Moreover, management tells you that you can't simply turn those users off -- these *are* paying customers we're talking about after all!! (and how much revenue comes in from those folks who are complaining about getting spammed, hmm?)
- As spam overwhelms many ISP abuse desks, a culture of ignoring **all** security problems arises; spam and other security problems seem to track very well.

A Data Point: Spamhaus.org' Top 10 Worst Spam ISPs June 2004

- #1 **MCI** (US): 195 entries
  #2 **Kornet.net**: 123 entries
  #3 **Savvis** (US): 122 entries
  #4 **Chinanet-CQ**: 110 entries
  #5 **Chinanet-GD**: 105 entries
  #6 **Above.net** (US): 94 entries
  #7 **Comcast** (US): 82 entries
  #8 **Interbusiness.it**: 74 entries
  #9 **Level3** (US): 71 entries
  #10 **Verizon.net** (US): 61 entries

More Data Points: Reputation Databases

- http://www.senderbase.org/ provides email volume estimates for domains and top sending IP addresses. Some of the names you'll recognize, some you won't.
- http://www.mynetwatchman.com/ provides information about activity seen by its distributed network of sensors, as does SAN's Internet Storm Center Source Report (http://isc.sans.org/source_report.php)
- http://www.openrbl.org/
- http://www.spamcop.net/

Another Data Point: Understanding the China Problem

- ‘Five countries are hosting the overwhelming majority - a staggering 99.68 per cent - of spammer websites, according to a study out yesterday [e.g., June 30th, 2004]

  ‘Most spam that arrives in email boxes contains a URL to a website within an email, to allow users to buy spamvertised products online. While 49 countries around the world are hosting spammer websites, unethical hosting firms overwhelmingly operate from just a few global hotspots. Anti-spam vendors Commtouch reckons 73.58 per cent of the websites referenced within spam sent last month were hosted in China, a 4.5 per cent decrease from May. South Korea (10.91 per cent), the United States (9.47 per cent), the Russian Federation (3.5 per cent) and Brazil (2.23 per cent) made up the remainder of the "Axis of Spam".’
  http://www.theregister.co.uk/2004/07/01/commtouch_spam_survey/

- China Anti-Spam Workshop Trip Report
  http://www.brandenburg.com/reports/200404-isc-trip-report.htm

User Socialization

User Socialization

- Beyond technical spam reporting, the other thing that you really should be doing is "socializing" your email users. By this, I mean your users need to understand:
  -- not everyone reads their email via a web browser; politeness implies that plain text (not html) is the correct way to go
  -- sending a 20MB attachment isn't something that all correspondents love getting, nor does "everyone" use Word/Excel/etc.

User Socialization (2)

- -- "Vacation" auto responders are almost always a bad idea and are seldom needed
  -- Sig files should be brief, if used at all
  -- Just because you have the technical ability (or the political clout) to send email to everyone on campus doesn't mean that you should ("intraspam" can be a real problem at some campuses)
- Helping your local users develop a culture of responsible email usage is part of getting mail back to "the way it used to be…"

The Importance Of Users Having Healthy Skepticism

- The other thing you need to inculcate in your users is a sense of healthy skepticism:
  -- No, you do not need to "verify" your Visa information or your eBay/PayPal password.
  -- No, there aren't millions of dollars waiting to be shared with you in Nigeria. Really.
  -- No, our staff would never ask you to email them your account password.
- Healthily skeptical users are robustly resistant to phishing and online scam spams.

Grizzled Veterans Survive The Stress Of The Spam War Well

- The process of helping users become somewhat worldly and healthily skeptical is also an important component of preparing them to wage war on spam. Fighting spam can require a somewhat thick skin as you deal with disgusting message topics, and a high level of motivation as you combat an unseen and constantly morphing enemy. Skeptical/cynical "battle hardened" users are well equipped to meet those challenges.

Is There Anything We DON'T Want Our Users To Do?

- Yes. For example, we don't want them to take direct retaliatory action since they may end up mailbombing or ping flooding an innocent party who is being "Joe jobbed."
- We don't want our users to munge their address (doesn't work, can cause all sorts of support issues if done ineptly).
- We don't want users to just give up.
- We don't want users to try to intentionally solicit more spam "just for us to block." :-)

Allowing Users to Opt Out of Filtering

Be Sure You Allow Users to Opt Out of Your Default Spam Filtering

- As a "pressure relief" valve, be sure to have a mechanism that allows users to opt out of your default spam filtering should they want to do so.
- Here at UO, users can create a .spamme file in their home directory (either from the shell prompt or via a web-based request form) to signal that they "want out" of our default spam filtering. Every hour we look for those files, and adjust filters accordingly
- (That same page can be used to re-enable filtering, too.) See: cc.uoregon.edu/cnews/winter2004/optout.html

Given the Chance, Do People Opt Out of Default Filtering?

- If you do a good job of filtering, requests to opt out of default system-wide filtering will be rare.
- As of 7/16/04 here at UO….
  -- 13 of 31849 UO student accounts have opted out of our default spam filtering (0.04% opt out rate)
  -- 85 of 14559 faculty/staff accounts (including role accounts, email aliases and mailing lists) have opted out (0. 58% opt out rate)

A Policy Choice:
Should Spam Filtering Be
On or Off By Default?

Given Those Sort of Numbers, Spam Filtering Is (and Should Be) Enabled By Default

- Assume that 99% of all users are irritated by spam, want it to go away, and will either welcome spam filtering or be ambivalent about its presence.
- If you have 20,000 users, that implies you can either make 19,800 users "opt-in" to optional filtering or you can make 200 users "opt-out" of default filtering. (So why do so many sites make spam filtering optional?)

Since This Isn't Lunchtime, An Analogy to Drive Home the Point

- *Assume you're running a restaurant that has a fly-in-the-soup problem.*

  You can make thousands of customer ask to have the flies in their soup removed, or you can have the one guy in a million who LIKES flies in soup ask to have the flies left in. Which makes the most sense?

Spam Filtering Exceptions

There Are Some Accounts Which MUST NOT Be Filtered By Default

- While the default recommendation is, and should be, that accounts get spam filtered by default, there are some accounts which by their very nature MUST NOT be filtered by default. Those accounts include RFC 2142-mandated abuse reporting addresses such as abuse@, postmaster@, etc.
- Check to see if your site is listed on http://www.rfc-ignorant.org/
- There are other exceptions, too…

For Example:
Admissions Inquiry Accounts

- For example, if we block some "spam" directed at our admissions office, might our admissions folks miss requests for information from potential enrollees? What's the net cost to the institution if we lose tuition revenue from ten (or a hundred) potential out of state students because we're blocking their inquiry email? [Estimated UO non-resident full time tuition and fees, 2003-2004, run $16,416 per academic year.]

Also Be Particularly Careful With Campus M.D.'s, Lawyers, etc.

- Under the Federal ECF (https://ecf.dcd.uscourts.gov/) email may now be used to transmit notices of legal pleadings. If email of that sort is sent to a University attorney and fails to get through, a default judgement may get entered when he/she misses a scheduled hearing.
- Or consider the patient of a teaching hospital surgeon who is unable to email her doc about her "chest pains," and then dies.

Filtering Port 25

See RFC3013 (“Recommended Internet Service Provider Security Services and Procedures”) at section 5.4

Spam From Just One Broadband Provider

- "Comcast users send out about 800 million messages a day [e.g., ~292 billion/year], but a mere 100 million flow through the company's official servers. **Almost all of the remaining 700 million [messages] represent spam**…" (http://news.com.com/2010-1034-5218178.html) (May 24, 2004)
- "On Monday [June 7, 2004], the company began targeting certain computers on its network of 5.7 million subscribers that appeared to be sending out large volumes of unsolicited e-mail. Spokeswoman Jeanne Russo said that in those cases, it is blocking what is known as port 25, a gateway used by computers to send e-mail to the Internet. The result, she said, was a 20 percent reduction in spam." http://www.washingtonpost.com/wp-dyn/articles/A35541-2004Jun11.html

Responsible ISPs Controlling Direct-to-MX Spam By Filtering Port 25

- As mentioned in the Comcast article, some responsible ISPs (and some universities) keep direct-to-MX spam (typically from open proxies or spam zombies) from leaving their networks by filtering port 25 (SMTP) traffic, allowing mail to be sent only via their official mail servers.
- Legitimate mail **can still be sent**, those messages just need to be sent via the official SMTP server the provider maintains.

Some Internet2 Schools Have Filtered Port 25, Either Campus-Wide or For a Subset of Users (or Have Plans to Do So)

- Buffalo: http://cit-helpdesk.buffalo.edu/services/faq/email.shtml#2.2.6
- CWRU: http://tiswww.case.edu/net/security/smtp-policy.html
- MIT: http://web.mit.edu/ist/topics/email/smtpauth/matrix.html
- Oregon State: http://oregonstate.edu/net/outages/index.php?action=view_single&outage_id=214
- TAMU: http://www.tamu.edu/network-services/smtp-relay/
- University of Florida: http://net-services.ufl.edu/security/public/email-std.shtml
- University of Maryland Baltimore County: http://www.umbc.edu/oit/resnet/faq.html#smtp-current-policy
- University of Missouri: http://iatservices.missouri.edu/security/road-map.html#port-25 (as of June 30, 2004)
- WPI: http://www.wpi.edu/Admin/IT/News/networkingnews.html#newsitem1059685336,32099,

If You *Do* Decide to Filter Port 25…

- If you *do* decide to filter port 25 traffic (except for traffic from your authorized SMTP servers), be sure you filter outbound AND inbound port 25 traffic. Why? Spoofed traffic from spammers "dual-homed" to a colo/dsl/cable ISP plus your compromised host/dialup, and who are sourcing packets from the colo/dsl/cable ISP with your compromised host's/dialup's IP addr.
- If you really want to lock down unauthorized mail servers, be sure to also pay attention to 465/tcp (SMTPS) and 587/tcp (see RFC2476), and also plan/decide how you'll handle travelers (VPNs?)

DNS “Hinting”

An Alternative to Locally Filtering Port 25

- One alternative to locally filtering port 25 is "hinting" (via ptr/in-addr DNS entries) about groups of hosts that should probably not be sending email "direct-to-MX." For example:

  *.wireless.indiana.edu
  *.user.msu.edu
  *.resnet.purdue.edu
  *.dhcp.vt.edu

  Folks "out there" can then block smtp from those sort of hosts (or not) as they deem appropriate.
- Avoid DNS naming schemes that require "mid-string" wildcarding (dialup67.example.edu)

DNS "Hinting" is Becoming Common in the Commercial ISP Space…

*.adsl-dhcp.tele.dk

*.cable.mindspring.com

*.client.comcast.net

*.customer.centurytel.net

*.dial.proxad.net

*.dsl.att.net

*.dynamic.covad.net

*.ppp.tpnet.pl

- Consistent naming would be nice (but isn't likely)

A Gotcha Some DSL Users May Run Into:

- 1) They register a vanity domain and point that domain at their DSL connection, BUT
  2) They fail to create a corresponding PTR (reverse DNS number-to-name) record, and
  3) They fail to route their outbound email through their provider's SMTP server.
- These guys get blocked when their server's address resolves to <foo>.dsl.<bar>.com rather than the vanity domain.
- They need to fix their reverse DNS or they need to use their provider's SMTP server

SPF

Another Option: Sender Policy Framework

- SPF allows mail servers to identify and block forged envelope senders (forged "Return-path addresses") early in the SMTP dialog by doing a simple DNS-based check of a site's text record.
- *Many* major providers/clueful sites are now publishing SPF records, including American University, AOL (~24.7M subscribers), Columbia, Delaware, Google, GNU.org, Iowa State, Lehigh, Oreilly.com, Oxford.ac.uk, Outblaze (>30M accounts), perl.org, SAP.com, South Carolina, spamhaus.org, w3.org, symantec.com, UCSD, etc. What about <u>your</u> university? `host -t txt example.edu`

SPF Implementation Issues

- Note that adoption of SPF can be done "asymmetrically" – you can publish your own SPF record but not query others, or vice versa.
- If you're used to email forwarding, get used to email rewriting (see the FAQ mentioned below)
- Roaming users will develop a sudden interest in VPNs and/or authenticated remote access
- You should know that here are competing approaches (such as MS's Caller-ID). SPF implementations can also do Caller-ID queries
- Want more information? http://spf.pobox.com/ (the FAQ there is particularly helpful)

Loss of Deliverability

Protect Your Deliverability (to AOL Users and Elsewhere)

- Important mail that you send to your students and other folks may not be getting through…

-- "[…] mail sent via UCLink/Listlink mailing lists to yahoo.com addresses is being blocked." http://www-uclink.berkeley.edu/ cgi-bin/display/news

-- "For several months, [Duke] was unable to send and receive e-mails to and from China…" http://www.chronicle.duke.edu/vnews/display.v/ART/2004/01/16/4007df2ebfe88

-- "Mail from IU to AOL blocked" http://www.bus.indiana.edu/news/ViewNews_Items_Details.asp?newsitemid=471&newsareaid=6

-- "After receiving a report indicating that no RAMS (Rutgers Automated Mass-mailing System) email messages were apparently making it into hotmail mailboxes, we decided to do a quick check to see if this was indeed true. Sure enough, the mail was not delivered to the mailbox with standard (default) mail filter settings in place." http://camden-www.rutgers.edu/RUCS-Camden/Announce/newsspring.04.hotmaillink.html

AOL Scomps

- One easy way to see if your users are emitting problematic email is to ask to receive AOL "scomps" (spam complaint reports) for your network blocks. See: http://www.nanog.org/mtg-0310/spam.html
- Caution: you may have infested systems that are spamming AOL users (and ONLY AOL users) which you're unaware exist. If you haven't been getting scomp reports previously, beware, the initial volume may be a little overwhelming…
- I have reason to believe that other major ISPs will soon begin offering scomp-like spam reports

Secure Your Own Servers/Networks

- We all know that insecure hosts, open SMTP relays, open proxy servers, exploitable formmail scripts, insecure ethernet ports and open wireless access points are *Bad Things*, right?
- Improving server security is now a global issue: http://www.ftc.gov/opa/2004/01/opsecure.htm
- Are you running a security scanner/auditing tool such as Nessus (http://www.nessus.org/)?
- Are you running a network intrusion detection system such as Snort (http://www.snort.org/) or Bro (http://www.icir.org/vern/bro-info.html)?

Other Things to Check/Do to Preserve Your University's Email Deliverability

- Are your mail servers on any DNSBLs? Check http://www.openrbl.org/
- Are your hosts showing up in SANS reports? Drill down at http://isc.sans.org/reports.html
- Do you have an RFC 2142-compliant abuse@ reporting address, or are you listed on http://www.rfc-ignorant.org/
- Are you purchasing connectivity from spammer-friendly ISPs? See http://www.spamhaus.org/sbl
- Do your mailings follow emerging industry standards? http://www.isipp.org/standards.php

If You Offer Institutional Mailing Lists…

- All subscriptions to mailing lists must be confirmed by the requesting subscriber
- Do NOT involuntarily put ANY users on ANY list (beware of the threat of "intraspam"!)
- Anything except plain text that gets sent to a list should get stripped
- Set list defaults to be reply-to-sender rather than reply-to-list by default
- Prevent random harvesting of list memberships
- Be sure to prevent harvesting of any online email directory you may offer, too!

And If Your Company Does Routinely Do Large Mailings…

- Be sure your mailings comply with emerging industry practices (see, e.g., http://www.isipp.org/standards.php)
- Consider trying BondedSender (https://www.bondedsender.com/)
- "Test send" your draft messages to a user who is running SpamAssassin (see http://www.spamassassin.org/)
- BE SURE your mailings comply with the letter and the spirit of all antispam laws.

Emerging Trends

Some Have Found Blocking Packets Rather Than Just Mail to Be Effective

- AOL blocks spammers' web sites
  http://www.washingtonpost.com/wp-dyn/articles/A9449-2004Mar19.html

  "America Online Inc. has adopted a new tactic against spam: blocking its members' ability to see Web sites promoted by bulk e-mailers."

- AOL reports drops in both e-mail & spam volume
  http://www.clickz.com/news/article.php/3328841

  "From Feb. 20th to March 17 […] AOL delivered 37 percent fewer e-mails to spam folders, from 178 million to 113 million. Member spam complaints dropped by 47 percent, from 12.4 million to 6.8 million."

Tarpits

- Tarpits are designed to drive spammers crazy by responding verrry slowwwllly to connections that are made to the tarpit'd host. If you're interested in exploring this as an amusing sideline, see:

  http://www.benzedrine.cx/relaydb.html

Proxypots

- Proxypots are another sort of trap some are using to counter spammers.
- Proxypots appear to be an open relay or open proxy, but in reality they are well instrumented systems that are carefully logging the origin of the spam that's being pumped through them. A nice example of a proxypot (complete with detailed data on abusers) is at: http://www.proxypot.org/reports/pacman/

.mail TLD

- Legitimate mail senders should also be aware that Spamhaus.org has floated a proposal to ICANN to create a new .mail TLD that would make it possible for trusted senders to be distinguished from spammers.
- See: http://www.spamhaus.org/tld/index.html and http://www.icann.org/tlds/stld-apps-19mar04/stld-public-comments.htm for more information.
- Obligatory disclosure: I've been named as the higher ed rep for the .mail Board of Directors.

Conclusion

In Conclusion: UO's Really A Very Typical University

- UO's really a very typical liberal arts state university of about 20,000 students.
- We face the same staff, financial and technical constraints that you face.
- We have a normal research university's academic faculty (with normal research university faculty expectations)
- SO… if we can do something locally about spam, so can YOU!