Email Effective Security Practices: 5 Concrete Areas To Scrutinize

Internet2 Member Meeting
Arlington VA, April 20, 2004

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

http://darkwing.uoregon.edu/~joe/emailsecurity/

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.
- Our goal is to highlight five concrete areas to scrutinize during our ten minute long slot.
- We’ll assume a Unix-based email environment.

#1: Encrypt Your POP & IMAP Traffic

- Hacker/crackers *love* to sniff 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.
- 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 at http://micro.uoregon.edu/security/email/)
- If you are NOT requiring encrypted POP and IMAP logins, the time has come to do so.

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
- Encourage use of GPG (http://www.gnupg.org/)

SMTP Auth With STARTTLS

- While you're encrypting POP and IMAP traffic, you might as well also require SMTP Auth (RFC 2554) over a TLS encrypted channel as well. 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!

#2. 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.

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.
- Faculty, staff and students must use an desktop A/V product at work and at home (see free home options at: http://www.pcworld.com/howto/article/0,aid,113462,tk,wb122403x,00.asp)

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.
- Recent estimates are that ~5% of hosts may be infested (See: http://www.newscientist.com/news/news.jsp?id=ns99994745).
- Antispyware reviewed: http://www.pcmag.com/article2/0,1759,1523357,00.asp (2 Mar 2004)

Your Users Should Also…

- Be running a current version of MS Windows, or an alternative OS (MacOS X, Linux, *BSD, etc.)
- Apply all available service packs and critical updates (check for updates to MS Office, too!); enable automatic Windows Updates.
- Use a personal software/hardware firewall
- Users should routinely backup their system
- Consider a system file integrity checker (cc.uoregon.edu/cnews/fall2003/sysintegrity.html)
- Use a strong password for their desktop system (particularly for Administrator accounts!)
- Avoid using risky applications (P2P, IM, etc.)

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)?
  -- See http://www.columbia.edu/kermit/safe.html

#3. Manage Spam (Yes, Spam *IS* a Security Issue)

- You probably are already taking steps to control spam, simply because spam now typically amounts to 75% of inbound mail (see: http://www.postini.com), however spam is also a security issue. See:
  -- "Your computer could be a 'spam zombie'" http://www.cnn.com/2004/TECH/ptech/02/17/spam.zombies.ap/
  -- "Spammers, Hackers Increasingly Feed Off Each Other" http://www.techweb.com/wire/story/TWB20040212S0009

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

- 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 filed in a spam folder, while messages that look non-spammy get delivered to the user's inbox.
- The biggest issues with SpamAssassin are (1) it requires that all messages first be accepted, then assessed and filed or discarded, (2) it relies on publicly-disclosed message characteristic heuristics for its filtering efficacy, and (3) it may be too hard for non-techy users.

DNS Black Lists

- The alternative approach, which we prefer and recommend, focuses on where messages are from.
- Message from a known spam source? Message from a known open relay or other insecure host? Block that traffic when the bad host tries to connect
- Sites using DNSBLs often use run multiple lists, such as MAPS RBL+ (http://www.mail-abuse.org/), Spamhaus SBL+XBL (http://www.spamhaus.org/), and NJABL (http://www.njabl.org/)
- Arrange to download and run copies of any DNSBL zones you use on your own local DNS servers.
- www.oag.state.tx.us/oagnews/release.php?id=413
- Tarpit info… http://www.benzedrine.cx/relaydb.html

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
- If you do a good job of filtering, usage will be rare: as of 3/30/2004, 7 of 30727 UO student accounts have opted out, as have 38 of 13151 faculty/staff (plus 5 role accounts and 10 mailing lists)

AOL's Latest Anti-Spam Technique (Controversial, But Apparently 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."

#4. 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? (c.f. http://darkwing.uoregon.edu/~joe/jt-proxies/)
- 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!

#5. What About Filtering Port 25?

- It is increasingly common among commercial broadband ISPs to filter customer port 25 traffic, forcing all inbound or outbound email to go through the provider's canonical SMTP servers. By doing this, "direct-to-MX" spam from infected computers can be prevented, and infected customers can be identified from their message volume, and promptly disabled.
- This sort of filtering of port 25 is explicitly discussed in RFC3013 ("Recommended Internet Service Provider Security Services and Procedures") at section 5.4

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?)

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)

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 AOL (~24.7M subscribers), Google, GNU.org, Oreilly.com, Oxford.ac.uk, Outblaze (>30M accounts), perl.org, SAP.com, spamhaus.org, w3.org, symantec.com, 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)

Thanks For the Chance to Talk Today!

- Are there any questions?