Top Messaging Vulnerabilities

Part 1 – Technical Issues

By Kevin Beaver, CISSP

Founder and principal consultant - Principle Logic, LLC

4430 Wade Green Rd., Suite 180

Kennesaw, GA 30144

kbeaver@principlelogic.com

www.principlelogic.com

Principle Logic

Your Answer to Information Security™

About Your Presenter – Kevin Beaver

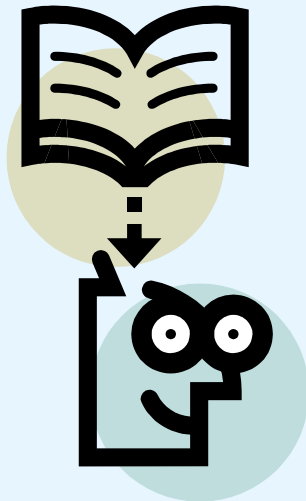
- Information security advisor, author, and trainer
- 16+ years experience in IT and specializes in information security assessments and incident response
- Author of the new book **Hacking For Dummies**
- Author of the *free* ebook **The Definitive Guide to Email Management and Security** (Realtimepublishers.com)
- Co-author of the new book **The Practical Guide to HIPAA Privacy and Security Compliance** (Auerbach Publications)
- Regular columnist and information security advisor for SearchExchange.com, SearchSecurity.com, SearchNetworking.com, and SearchWindowsSecurity.com
- Bachelor's in Computer Engineering Technology from Southern Poly & Master's in Management of Technology from Georgia Tech
- Holds CISSP, MCSE, MCNE, and IT Project+ certifications

Principle Logic

Your Answer to Information Security™

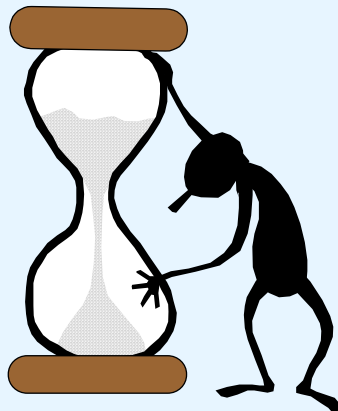
What You'll Learn Today

- Common technical security vulnerabilities I see all the time in email and instant messaging systems
- Practical (simple and often free) countermeasures you can implement now



Common Mistakes

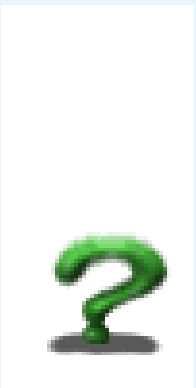
- Take security of messaging systems for granted
- Haven't realized the level of confidential information that flows through these systems
- Believe that malware protection and encryption are all that's needed
- Ignore – or just can't keep up with – all the new vulnerabilities and patches
- Have tough policies with no enforcement



Why highlight messaging systems?

- Technology is certainly not sexy*!*
- Everyone's doing it

  …and have been for a long time
- Mostly widely used business app
- It's not just for sending messages any more
- One of the most commonly exploited systems



Why are messaging systems insecure?

- Old protocols designed w/o security in mind
- Convenience and usability *far* outweigh the demand for security
- Underlying OS/network issues often forgotten
- Applications allow too much end user control
  - See 2nd bullet above

How Messaging Attacks Are Carried Out

Most attacks are actually pretty simple

- Malware taking systems down, deleting data, and even extracting confidential info
- Exploiting OS and other vulnerabilities to obtain remote control and more
- Cracking into unencrypted message stores and log files
- Capturing data in transit and viewing it in clear text

DoS Attacks

- Email bombs
- Attachment overloads
- Auto-responder attacks

Some Solutions

- Throttle connections
- Limit/filter file attachments
- Don’t allow out of office replies

Banner Grabbing

- Discloses important version information
- General lack of banner warning information
- Even if you do, changing banners isn't foolproof

Some Solutions

- Change defaults
- Keep systems hardened patched
- Use an email firewall or proxy
- Use warning banners

SMTP Attacks

- Account enumeration via EXPN/VRFY commands
- Email header disclosures
- Open relays

Some Solutions

- Disable/limit EXPN and VRFY commands
- Check headers and re-write them if necessary
- Enforce SMTP authentication
- Close open relays!

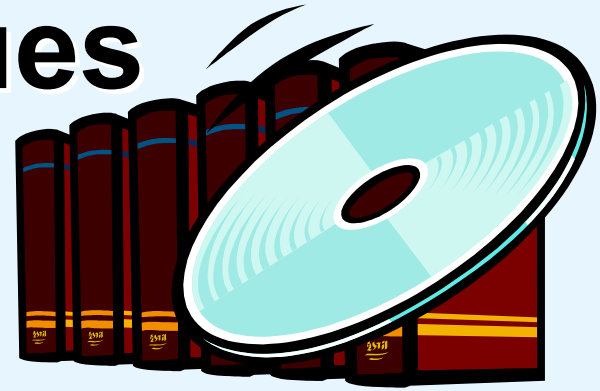
Clear Text Messages

- Most email goes across the wire/air in clear text
- Can disclose IP & provide ways to hack other hosts
- Message stores & log files are even more vulnerable

<u>Some Solutions</u>

- Use switches (not foolproof!) and IDS/IDP
- Encrypt – preferably at the server/perimeter
- Use a system that encrypts message store
- Disable/limit logging if you don't use it

Storage Issues



- Running out of storage space
- Lack of fault-tolerance

Some Solutions

- Limit storage space…just beware !
- Implement failover systems

Spam?

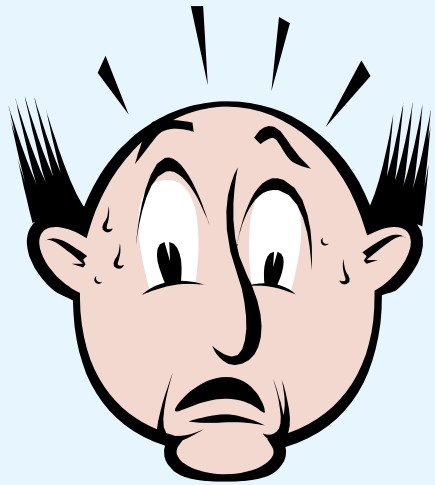
- Eats up bandwidth and storage space
  - DoS anyone?
- Potential for malware attachments
- Chance of your own systems being blacklisted
- Diverts security resources from more important issues

<u>Some Solutions</u>

- Use a mix of various filtering methods
- Filter at the server/perimeter mostly
- Resort to whitelists or stop using email?

Vulnerable Hosts

- Must allow both inbound and outbound traffic
- Firewalls offer limited protection
- Other apps running on hosts can open new holes and create stability issues
- Web servers for web access
- Passwords?



<u>Some Solutions</u>

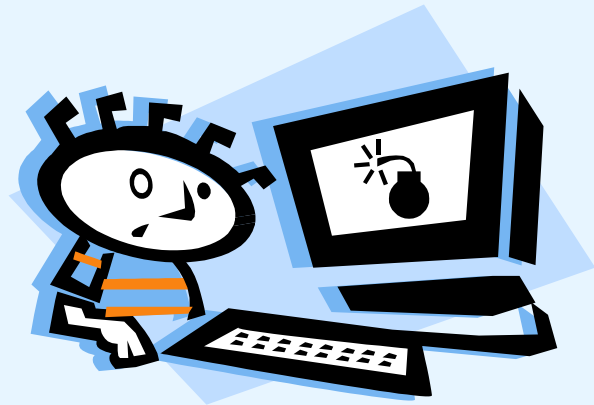
- Harden your hosts
- Email firewalls help – just don't bypass host security
- Use dedicated servers
- Passwords? ….well…

Instant Messaging Flaws

- Users can easily share any drive
- New channel for malware
- Some vulnerabilities have enabled remote control
- Serious log file issues – especially if a host is compromised or stolen

<u>Some Solutions</u>

- Don’t give users control!
- Use a more robust IM solution
- Use IM content filtering and firewalls

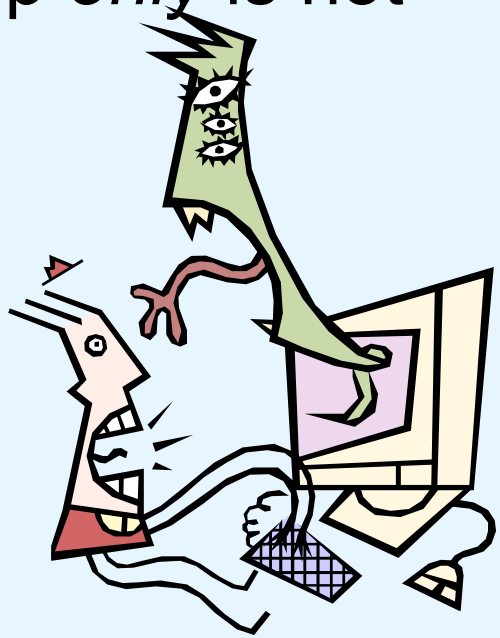


…and Malware (of course)

- Messaging is the preferred method of travel
- Virus signatures and engines out of date
- Services running that aren't needed are often compromised
- Relying on protection at the desktop *only* is not good!

<u>Some Solutions</u>

- *Centralized* malware protection
- Consider behavioral protection
- Use multiple layers and engines



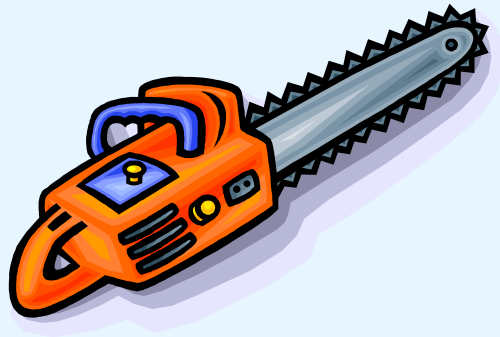
Other Cool Countermeasures

- Implement technical security measures as close to the network perimeter & as far away from users as possible
- Use PGP or S/MIME for standalone encryption
- If practical…email firewalls work great
  - Consider IM protection as well
- Don't rely on technical security measures alone!

Don't…

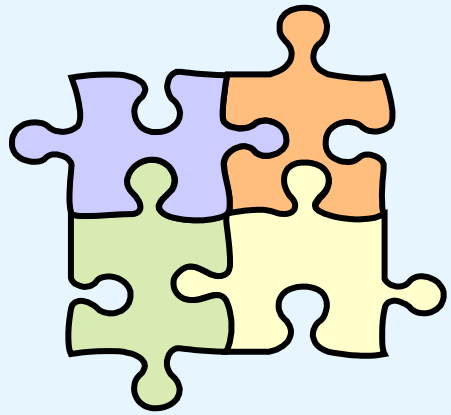
- Think that messaging vulnerabilities are important just because it's not sexy
- Think that email is less vulnerable than your other systems
- Assume that if no issues are found when testing that none exist now or will in the future

Tools



- Test for open relays
  - www.abuse.net/relay.html
- Email security test
  - www.gfi.com/emailsecuritytest
- SMTPScan to see what the bad guys can see
  - www.greyhats.org/outils/smtpscan
- Spam lookup and other email tests
  - www.dnsstuff.com

Resources



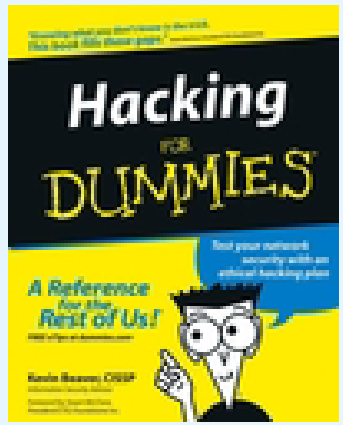
Vulnerability Databases

- NIST ICAT Metabase
  - http://icat.nist.gov/icat.cfm
- Common Vulnerabilities and Exposures
  - www.cve.mitre.org/cve

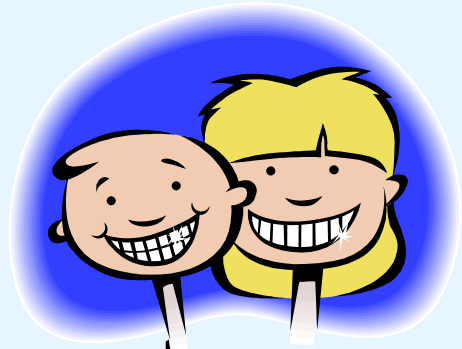
System Hardening

- NSA Configuration Guides
  - www.nsa.gov/snac
- Guide on disabling open relays
  www.mailabuse.org/tsi/ar-fix.html

My in-depth testing techniques in *Hacking For Dummies*



Wrap Up



Remember that…

- Technical security issues in messaging systems must remain on your security shortlist
  - Test them as you would web servers, file servers, OSs, & other critical systems
- Your network is only as secure as your weakest system – don't let email be the point of entry
  - Vice versa
- A *pound* of prevention is worth a **ton** of cure
- Keep It Simple, Somebody!

Thanks for joining me!

Principle Logic

Your Answer to Information Security℠