Information Security 101: Security Essentials at UH

Jodi Ito
Information Technology Services
jodi@hawaii.edu
Why is security important?

“We’re not in Kansas anymore, Toto!”
Role of Computers Today

- Use computers and networks daily
- Protect systems and resources
- Protect information
- Security is as strong as the weakest link
- But needs to be balanced against usability
Security is EVERYONE’S Responsibility!
Today’s Agenda

- Recommendations for Desktop Computers
- Recommendations for System and Network Administrators
- Things that ITS is considering
General Recommendations

- Physical Security
  - Turn off systems at night/weekends
  - Do not leave systems logged-in unattended
  - Use locking screen savers
    - Built-in Windows
    - Blackwatch for Macs
      (penumbra.apple.com/blackwatch.html)
Passwords

- Select “good” passwords
  - Avoid: “dictionary” words, any part of your name or ID
  - Include: upper/lowercase, numbers, special characters
  - PgPtH2b! (Pick good Passwords that are Hard 2 Break!)

- Change passwords frequently
Don’t write passwords down!
More Recommendations

- Backup your system and data
- Encrypt sensitive information
- Stay informed
  - Subscribe to informational mailing lists
  - Check vendor and security organization sites regularly
  - Talk w/ your colleagues
Encryption

- Use to encrypt email and sensitive data
- PGP from MIT
  - web.mit.edu/network/pgp.html
- Available for all operating systems
  - Windows 95/95/NT/2000
  - MacOS 7.6.1 and higher
  - AIX/HP-UX, Linux, Solaris
Operating Systems

- Install latest patches
- Turn off non-essential services
- Change default passwords
- Questions about Windows NT/2000:
  w2k-help@hawaii.edu
- Other questions:
  help@hawaii.edu
Virus Protection

- Install latest version of anti-virus software
- Install latest virus definition files
- Install software on ALL systems
- UH site license for anti-virus software
  - For both office and home use
  - Subscribe to uhvirus-alert@hawaii.edu
  - Check vendor websites (NAI, Norton, etc.)
Email

- Do not open attachments automatically
- Do not open attachments from unknown sources
- Do not open unexpected attachments
- Turn off any “preview” options
- Scan attachments (with current anti-virus software) BEFORE opening
- MS Outlook vulnerabilities
Personal Firewalls

- What is it?
- Why do I need one?
- Where do I get one?
- ITS status on recommendations
What is a “Personal Firewall”?

- Software that monitors & logs activity on your computer
- Can track both incoming and outgoing traffic
When do I need a firewall?

- Computers are easily accessible through networks
- Computers are “always on”
  - DSL, cable modems, offices
- Susceptible to intrusions, viruses, trojan horses
- Distributed, zombie attacks becoming more popular
Products & Availability

- Commonly used products:
  - Black Ice Defender (www.networkice.com)
  - ZoneAlarm (www.zonelabs.com)
  - ConSeal PC (www.consealfirewall.com)
  - Hack Tracer (www.sharptech.com)

- Purchase or Download
- ITS is currently reviewing products
System and Network Administrators
General Recommendations

- Have a security policy
- Review and maintain the security policy
- Enforce strong passwords and expirations
- Keep logs and monitor for suspicious activities
- Review the SANS Top 10 list of vulnerabilities: www.sans.org
Server Issues

- Delete unused accounts
- Change passwords on default accounts
- Have Login/Password management strategy and enforce it
- Turn off all unnecessary services
More Server Issues

- Mail Servers: install latest patches to prevent anonymous mail relaying (prevent mail spamming)
  - sendmail Web site: www.sendmail.org
  - PMDF Web site (for smtp and IMAP/POP): www.innosoph.com
More Server Issues

- FTP Servers: disable anonymous, (potential software distribution site)
- Web servers: “deny then allow”, only allow admin access from console
  - www.w3.org/Security
Incident Reporting

- Send email to: security@hawaii.edu
- With:
  - Contact information (name, dept, phone)
  - Date & Time of activity
  - Operating System & version number
  - Type and severity of activity
  - Supporting documentation (logs, tool reports, etc.)
Tools

- Password crackers: crack, l0pht crack
- Host-based IDS: tcpwrappers, Norton Internet Security 2000, tripwire
- Network-based IDS: ISS RealSecure, SNORT, tcpdump
- Vulnerability Assessment Tools: SAINT, CyberCop, nmap
- System Audits: system file checker
- File integrity checkers: tripwire
Top 50 Tools URL

- www.insecure.org/tools.html
WARNING!

Do NOT run these on or against systems or networks that you do not administer!

(unless you have explicit permission from the system or network administrator AND notified users in advance!)
ITS Considerations*

- No shell accounts after July 2001
- Require use of SSH for shell logins
- Enforce stronger passwords AND password expirations
- Standardize on PGP for transmission of sensitive information
- Install enterprise mail virus scanner
* ITS is currently reviewing these for possible adoption and implementation.
Resources

- www.sans.org
- www.nai.com
- www.norton.com
- www.ciac.org
- security.vt.edu
- www.cert.org
- www.abuse.net
- www.doshelp.com
More Resources

- www.stanford.edu/group/itss-ccs/security
- www.advisor.com/mis
- www.nwc.com
- www.securityfocus.com
Questions?

jodi@hawaii.edu
956-2400