A Windows Desktop Security Primer

ITSS Technical Briefing

Jay Stamps, ITSS, jstamps@stanford.edu, 723-0018
Turing Auditorium, May 20, 2005
Topics for the Afternoon

- Windows XP Professional Security
- Setting Up a New PC Safely
- Secure Windows Configuration
- Software Tools for Better Security
- Good Security Practices for You
- Passwords vs. Pass Phrases
- “Malware” and “Phishing” Scams
- Windows Security Top 10 List
- What to Look Forward To
- Other Security Resources
Speaking of Computers, etc.

- Stanford University Libraries Publication
  - Three issues each year (Fall, Winter, Spring)
  - To subscribe to Speaking of Computers:
    http://speaking.stanford.edu/subscribe.html

- Windows Security Article (Spring 2005):
  http://speaking.stanford.edu/highlights/Make_Your_PC_Secure.html

- Friday Tech Briefings Web Site:
  http://www.stanford.edu/services/techtraining/techbriefings/
  - To subscribe to the Tech Briefings mailing list:
    http://www.stanford.edu/services/techtraining/techbriefings/#list
Important Updates on ESS

◆ Symantec AntiVirus 9.0.3 Is on ESS
  ◆ The previous ESS distribution is threatened
    ◆ http://www.stanford.edu/~jstamps/SAV_repair.html

◆ Eudora <= 6.2.0 for Windows Is Vulnerable
  ◆ http://www.eudora.com/security.html
  ◆ http://www.ngssoftware.com/advisories/eudora-01.txt
  ◆ http://www.stanford.edu/dept/itss/ess/pc/eudora.html

◆ ITSS Microsoft Office Patcher Redux
  ◆ Critical vulnerability in MS Office XP (et al.)
    ◆ http://www.microsoft.com/technet/security/bulletin/ms05-005.mspx
  ◆ ITSS MS Office Patcher is here:
    ◆ http://www.stanford.edu/dept/itss/ess/pc/msoffice_patcher.html

◆ PC-Leland 2.1.4.7 Is on ESS
Windows XP Pro Security

- **What We Will Talk About**
  - Windows XP Professional Security
  - Advice applies to non-English editions, too
  - Focus on stand-alone PCs attached to SUNet

- **What We Won’t Talk About** (after this slide…)
  - Windows XP Home Edition
  - Mac OS X, Linux, Unix, Palm OS, etc.

- **But Don’t Walk Out Just Yet!**
  - Some of my advice may apply to other OSes
  - PC users should consider upgrading to XP Pro
What’s the Threat?

◆ Viruses, Hackers and Worms - Oh, My!
  ◆ Purists reserve the term “hacker” for ace programmers, not “attackers”
    http://catb.org/~esr/jargon/html/H/hacker.html

◆ “Virus” is also an overworked term
  ◆ Internet worms, mass-mailing worms, viruses (infectors), Trojan Horses, backdoors, rootkits, bots, zombie networks, spyware, hijacking…
  ◆ The best general term is “malware”

◆ You Get the Idea: It’s a Jungle Out There!
  ◆ And an oz. of protection is worth a lb. of cure
A Little Caveat

- Some of You Have Local Technical Support Staff
- Some of You May Be Local Technical Support Staff
- A Quick Quiz Question: If I Say Something That Contradicts What Your Local Support Staff Say, You Should…
  A. Do what I say anyway
  B. Do what your local support folks say
  C. Talk to your local support staff
  D. Give up using computers: Too much hassle!
A Few Assumptions

- Much of What Follows Assumes That
  - You have administrator rights for your PC
  - Your PC is not a member of a Windows domain - though maybe it should be! See: http://windows.stanford.edu
  - If you have local technical support staff, you have their blessing to make changes to your PC’s configuration
  - You understand that changing security-related settings can impair functionality: You might have to undo some changes
User Rights & Privileges

◆ What Are “Administrator Rights”?
◆ A User in the Administrators Group
  ◆ Can modify or delete all files, including (with some protections) system files
  ◆ Can modify the Windows registry
  ◆ Can define local security policies
  ◆ Has more or less total control
◆ Because of How Windows Applications Are Designed, Administrator Rights Are Often Necessary for “Normal Use”
  ◆ Primary XP user has administrator rights
Out of the Box

- **You Just Got a New PC: Now What?**
  - It’s not securely configured by default
  - Security software is probably missing
  - The “survival time” of an unpatched PC

- **First: Don’t Put It on the Network!**
  - *Do* set strong passwords or pass phrases
  - *Do* disable File & Printer Sharing
  - *Do* enable the Windows Firewall

- **Configure Your Network Settings**
  - *Now* you can connect to the Internet
So You’re on the Internet...

- Go to http://windowsupdate.microsoft.com
  - Install all critical updates and service packs
  - Reboot and revisit the Windows Update site
  - Lather, rinse, repeat...
- Go to http://ess.stanford.edu
  - Stanford Essential Software: Gotta have it!
  - Download and install Symantec AntiVirus
    - Remove any previously installed AV software
    - Start | Settings | Control Panel | Add or Remove
  - Download and install SpySweeper
  - Download and install BigFix
  - Download and run the Security Self-Help tool
What’s All This, Then?
Summary of Demonstrations

◆ Symantec AntiVirus
  ◆ Schedule LiveUpdate to run daily
    ◆ You must have administrator rights
  ◆ Schedule full scans weekly
    ◆ Scheduled scans are specific to user accounts
  ◆ If you use Eudora see:
    http://securecomputing.stanford.edu/sav/index.html

◆ SpySweeper
  ◆ Requires administrator rights
  ◆ Read instructions; Configure weekly “sweeps”
  ◆ Restore “cookies” or “spyware” if required
  ◆ Try other anti-spyware programs
Summary of Demonstrations

- **BigFix Client Software**
  - Use to supplement Windows Auto Updates
  - Must be installed with administrator rights
  - Runs invisibly in background
  - Collects a little inventory information
    - Subscribe to bigfix-users@lists.stanford.edu
  - Supports all Windows platforms (& most languages)

- **Stanford Security Self-Help Tool**
  - Configures a number of important settings
    - Does *not* check your PC’s patch level!
  - Checks for blank or weak passwords
  - Configuration changes can be *undone*
A Note on “Service Pack 2”

◆ Windows XP Service Pack 2 Is Now Out
  ◆ Install on both Pro and Home Editions
  ◆ A number of important new security features
    ◆ For example, Data Execution Prevention - see: [http://support.microsoft.com/default.aspx?scid=kb;en-us;875352](http://support.microsoft.com/default.aspx?scid=kb;en-us;875352)
  ◆ May change Windows’ behavior noticeably

◆ Download the XP SP2 Configuration Tool
  ◆ Available on the ESS site
  ◆ Will prevent problems with Internet Explorer for users of Stanford business applications

◆ Check Out David Pogue’s (copyrighted) *New York Times* Article on SP2:
  ◆ Use Google to search on *Pogue Windows SP2*
Pogue’s 7 Steps (Modified)

- Check Your Hard Drive for Free Space
- Remove Spyware & Scan for Viruses
- Visit the Windows Update Web Site
  - Install everything except SP2
- Visit Your PC Manufacturer’s Web Site
  - Download and run BIOS updater
- Back Up All Your Files, Including Hidden
- Remove Antivirus and 3rd-Party Firewalls
  - Enable XP’s built-in firewall first!
- Log Off Everyone But Yourself
Uninstalling SP2

- Installing Service Pack 2 Seldom Causes Problems
- But If It Does…
  - Go to Start | Settings | Control Panel | Add or Remove Programs
  - Look for “Windows XP Service Pack 2” and click the “Remove” button
  - Restart Windows
- Good Luck! But This Usually Works
Quick Tour 1: The WF

- The Service Pack 2 Windows Firewall
  - Successor to the Internet Connection Firewall
  - Deeply integrated, easily configurable
  - Doesn’t block outgoing network traffic
  - Can prompt you to open listening ports
  - Allows you to configure “exceptions”

- Some Other Personal Firewalls
  - Zone Lab’s ZoneAlarm
  - Symantec’s Norton Personal Firewall
  - Trend Micro’s PC-cillin Internet Security
  - ISS’s BlackICE PC Protection
Quick Tour 1: The WF

- Go to Start | Settings | Control Panel
- Click “Switch to Classic View”
- Double-click “Network Connections”
- Right-click “Local Area Connection”
- Choose Properties
- Click the Advanced Tab
- Click the “Settings…” Button
- Click the Exceptions Tab
- Use the “Add Program…” or “Add Port…” Button to Configure Exceptions
Quick Tour 1: The WF

In Windows XP SP2 you can go directly to the Windows Firewall control panel, found among all your other control panels.
Quick Tour 1: The WF

If you select a program or port under the Exceptions tab and click “Edit,” you can specify a “scope”: i.e., tell the firewall only to permit traffic from an IP address or range of addresses to the selected program or port. The externally routable network address space for most of SUNet is defined by

171.64.0.0/255.252.0.0

where 255.252.0.0 is the appropriate network mask.

Firewall exceptions apply to all network interfaces.
Quick Tour 2: User Accounts

- Ensure That All User Accounts Have Good Passwords or Pass Phrases
  - By default no remote logon with null password
- Go to Start | Settings | Control Panel
- Click “Switch to Classic View”
- Double-click “User Accounts”
- Click on a User Account by Name
- Choose “Create Password” or…
- To Change an Existing Password, Log in as User Whose Password Is to Be Changed
Quick Tour 2: User Accounts

- Not Available for Windows XP Home
- Go to Start | Settings | Control Panel
- Click “Switch to Classic View”
- Open “Administrative Tools” Folder
- Double-click “Computer Management”
- Click to Expand “Local Users and Groups”
- Click on Users Folder Icon
- Right-click Individual User Accounts by Name and Select “Properties”
- Disable Unneeded Accounts
Quick Tour 2: User Accounts
Quick Tour 3: Auto Updates

- Use Windows Automatic Updates
  - In conjunction with BigFix
- Go to Start | Settings | Control Panel
- Click “Switch to Classic View”
- Double-click Automatic Updates
- Select “Automatic”
- Choose “Every Day”
- Pick a Time When the PC Will Be On
  - But no one has to be logged in
- Click OK
Quick Tour 3: Auto Updates

Automatic Updates

Help protect your PC

Windows can regularly check for important updates and install them for you. (Turning on Automatic Updates may automatically update Windows Update software first, before any other updates.)

How does Automatic Updates work?

- **Automatic (recommended)**: Automatically download recommended updates for my computer and install them:
  - Every day
  - at 10:00 AM

- Download updates for me, but let me choose when to install them.
- Notify me but don't automatically download or install them.
- Turn off Automatic Updates.

Your computer will be more vulnerable unless you install updates regularly. Install updates from the [Windows Update Web site](#).

Offer updates again that I've previously hidden.

[OK]  [Cancel]  [Apply]
Note on Folder Views

- In Windows Explorer Go to Tools Menu
- Select “Folder Options…”
- Click the View Tab
- Select “Show hidden files and folders”
  - If you look inside the Documents and Settings folder, you’ll now be able to see folders that had been hidden previously
- Uncheck “Hide extensions for known file types”
- Click OK
Note on Folder Views

Folder Options dialog box showing settings for folder views and advanced settings.
Note on Windows File Sharing

- Always Disable Unneeded Services
- File & Printer Sharing Is an Open Door
- Go to Start | Settings | Control Panel
- Click “Switch to Classic View”
- Double-click “Network Connections”
- Right-click “Local Area Connection”
- Choose Properties
- Uncheck “File and Printer Sharing”
- Consider Using PC-AFS for File Sharing
  - http://filetransfer.stanford.edu
Note on Windows File Sharing
Encrypting File System

◆ Stanford Has No Central PKI
  ◆ That’s “Public Key Infrastructure”
  ◆ If something goes wrong, your encrypted data will probably be unrecoverable - *lost forever*

◆ Not Supported by XP Home

◆ 256-bit AES Encryption on >= XP SP1

◆ Use with Caution
  ◆ Back up your EFS certificate
  ◆ Win XP provides no default Recovery Agent
Encrypting File System

You should encrypt entire folders rather than individual files: All files in that folder will then automatically be encrypted. Right-click the folder you want to encrypt, select Properties from the contextual menu, and under the General tab click the “Advanced…” button. Click the check-box to “Encrypt contents to secure data” and then click the “OK” button.
Encrypting File System

Click the “OK” button to confirm. Note that the labels for encrypted files and folders will be green in color.
Passwords vs. Pass Phrases

- Security: A Tradeoff with Convenience
- Attacks against User Account Passwords
  - Dictionary, Brute-Force & Hybrid Attacks
  - Pre-Computed Hashes
- Password Complexity Is a Function of
  - Length, size of the symbol set, and ordering -
  - Thus, assuming a random ordering, for each additional character in a password, cracking becomes exponentially harder
- See This Speaking of Computers Article:
  [http://speaking.stanford.edu/highlights/Passwords_Are_Passe.html](http://speaking.stanford.edu/highlights/Passwords_Are_Passe.html)
Single Sign-On

- If You’ve Got a Really Good Pass Phrase, Why Waste It?
- By Logging in to Windows, You Can Also Log in to PC-Leland
- You Now Have *Carte Blanche* to Access Many Restricted Stanford Resources
- Configure PC-Leland
  - Right-click the PC-Leland System Tray icon
  - Choose “Settings…,” then Security
  - For instructions see the Security section of [http://www.stanford.edu/group/itss/pcleland/help/settings.htm](http://www.stanford.edu/group/itss/pcleland/help/settings.htm)
Malware & Phishing Scams

- Mass-Mailing Worms
  - Arrive as email attachments
  - Generally can’t be activated unless you open an infected attachment
  - Could be embedded in HTML messages

- Phishing Scams
  - Try very hard to look legitimate
    - International Domain Name spoofing doesn’t affect IE
  - Latest scams direct you to a phony web site to enter personal information - or else!
  - Don’t open unexpected attachments! or respond to unsolicited requests!
Spyware & Adware

- Spyware Tracks Web Browsing Habits
  - Some “adware” is “legitimate”
  - You have to read the fine print!
- Marketscore Brings a New Twist
- Browser Hijacking
  - You’ll notice if this happens to you!
- Be Wary of “Free” Software
  - That includes “security” software!
  - Also some alleged “antispyware” products
- Think Before You Click!
  - Web links, software downloads, etc.
Top 10 Security Measures

- Patch Microsoft Windows Automatically
  - New patches 2nd Tuesday of each month
  - Use BigFix & Windows Automatic Updates
- Use Strong Passwords (even better, pass phrases) for *All* User Accounts
- Use and Properly Maintain Good Antivirus Software
- Use a Firewall, such as Windows XP’s Built-in Software Firewall
- Don’t Open Suspicious Email Attachments or Respond to Suspicious Requests
Top 10 Security Measures

- Disable Windows File & Printer Sharing
  - So long as you’re not using these services
  - Disable in Local Area Connection Properties
- Disable Unneeded User Accounts
- Don’t Use Automatic Logon (off by default)
  - Less likely to forget your password!
    - [http://support.microsoft.com/default.aspx?scid=kb;en-us;315231](http://support.microsoft.com/default.aspx?scid=kb;en-us;315231)
- Use the Screen Lock When You Step Away & Shut Down When Gone for Over 6 Hours
- If Possible, Don’t Use Internet Explorer:
  - Try [http://www.mozilla.org/firefox](http://www.mozilla.org/firefox)
What’s Next?

- ITSS Is Working to Provide
  - Best practices documents for configuring
    - Windows
    - Mac OS X
  - Tools to help standardize configurations
  - Management tools (BigFix, for example)
    - BigFix will also help with asset tracking
  - Controlled Network Access
  - Greater user awareness of good computer security practices
  - Better self-help documentation and tools for ordinary computer users
Tools for Prevention

- **Essential Stanford Software**
  - [http://ess.stanford.edu](http://ess.stanford.edu)
  - Symantec AntiVirus
  - BigFix client ([http://patching.stanford.edu](http://patching.stanford.edu))
  - SpySweeper
  - Security Self-Help Tool

- Use the Firefox Web Browser (not IE)

- **Stanford Secure Computing Web Site**
  - [http://securecomputing.stanford.edu](http://securecomputing.stanford.edu)

- **Microsoft Baseline Security Analyzer**
  - [http://support.microsoft.com/kb/320454](http://support.microsoft.com/kb/320454)
More Help Resources

- **Networking Resources**
  - Connect your PC to SUNet
    http://www.stanford.edu/dept/itss/ess/pc/sunet.html
  - Stanford’s Netspeed web site
    http://netspeed.stanford.edu
  - http://helpme.stanford.edu
  - “Windows XP: Surviving the First Day”
    http://www.sans.org/rr/whitepapers/windows/1298.php

- Use Windows’ Built-in Help
  - Go to Start | Help and Support

- Check out http://www.sysinternals.com
Questions? Research Tools

◆ If You’ve Been Saving Up Questions, Now’s Your Chance!

◆ Malware Research & Troubleshooting:
  ◆ http://support.microsoft.com/kb/129972
  ◆ http://www.google.com
  ◆ http://www.sarc.com
  ◆ http://housecall.trendmicro.com/
  ◆ http://www.educause.edu/Browse/645?PARENT_ID=741
  ◆ http://www.spywareinfo.com/
  ◆ http://support.microsoft.com
  ◆ http://www.microsoft.com/technet
  ◆ http://www.cert.org/
  ◆ http://www.cisecurity.org/