Rebuilding and Hardening for Windows XP Professional

This guide is currently being revised. If you have any comments or questions, please feel free to contact abraham@caltech.edu
Introduction

This guide for rebuilding and hardening Windows XP Professional machines consists of two parts, and an appendix. The first part contains a number of critical steps which everybody should take in order to prevent being infected with currently common worms. Other than the initial installation of Windows and running Windows Update, the hardening steps as described in the first part should take less than 30 minutes to do. The second part consists of recommended changes, as well some additional tips and tweaks which you may or may not wish to take depending on your own situation. Critical steps are marked with a *Critical*, and suggested steps have a little blurb describing why you may or may not choose to implement the suggestion. The entire first part is considered critical.

The majority of the guide is targeted towards XP machines which are:

1. Not part of a domain,
2. Do not have a remote systems administrator,
3. Are not dual booting with another OS,
4. Not running any servers, and
5. Do not need to transfer files directly with Windows 95/98/ME machines.

Most of this guide is still applicable even if your computer does not fall cleanly into the above categories, but you may wish to be more careful when implementing some of the suggested steps. Any time you encounter an optional step which you are not familiar with, or not sure about the result of, you should check up on the results of the step before implementing it. While following this guide step for step will result in an XP system with greatly improved security, it is no substitute for ongoing attention to good computing security, including keeping up with patches, maintaining an up-to-date virus definition list, and exercising care with email attachments.

*Critical*  If you are rebuilding a machine, be sure to back up any data that you want to keep! Good choices for backing up include burning data onto CDs or DVDs, external hard drives, or tape drives. This guide assumes that you will be formatting your hard drive to perform a clean install of XP, which results in the loss of any data you may currently have on the hard drive.

As a side note, if you've recently purchased a machine from a major computer vendor (such as Dell), it probably came pre-installed with XP Home. We strongly recommend rebuilding with Windows XP using this guide. The only caveat is that you may wish to make sure that you can re-install any pre-installed software that you may wish to keep, either through a Caltech site-license (site licensed software can be found at http://software.caltech.edu or by having the original install disc.

Please direct any questions, comments, or suggestions to abraham@caltech.edu
Checklist *Critical*

Before you start on this guide, you should have:

1. A printed copy of this guide

2. Have the Windows XP Professional SR-1 installation disc on hand, as well as the registration codes.

   If you are Caltech faculty, staff, or postdoc, you can obtain the installation disc and registration code through either [http://software.caltech.edu](http://software.caltech.edu) or by going to the ITS Help Desk with your Caltech ID (x4602, open 8am-5pm M-F, closed noon-1pm).

   If you are a Caltech graduate student or undergraduate, you can obtain permission to download the installation disc image (.iso) by emailing software@its.caltech.edu

3. Have the latest Symantec AntiVirus (currently version 8.1) installation disc on hand. This can be obtained by all Caltech personnel through either [http://software.caltech.edu](http://software.caltech.edu) or by going to the ITS Help Desk with your Caltech ID (x4602, open 8am-5pm M-F, closed noon-1pm). We recommend that you install the Caltech site-licensed version of Symantec Anti-virus (AV) instead of any other anti-virus software you may already have, since the site-licensed AV does not expire.

   Please note that Symantec has also been known as Norton. For the sake of consistency throughout this guide, we will refer to the company and product as Symantec.

4. Have the latest virus definition files (aka Intelligent Updater) for Symantec burnt onto a CD or downloaded onto a USB jumpdrive. The latest virus definition files can be downloaded from [http://securityresponse.symantec.com/avcenter/defs.download.html](http://securityresponse.symantec.com/avcenter/defs.download.html) or obtained from the ITS Help Desk.

5. If you are rebuilding a machine, be sure to have backed up any of your old data before you start!

6. Make a note of your network settings before you rebuild, particularly with the following info:
   a. Static or DHCP IP address (if static, note the actual IP, as well as the gateway and subnet mask)
   b. DNS Server (typically 131.215.139.100 and 131.215.9.49)
   c. WINS Server (typically 131.215.220.220 and 131.215.51.51)
I. Rebuilding and Securing XP *Critical*  
*(All new rebuilds should go through these steps)*

1. Leave your network cable unplugged while initially installing XP. *Critical*  
   Depending on when you're rebuilding, you can get infected before you even log in the first time -- the record for fastest re-infection of a newly rebuilt machine during the highest point of MSBlaster activity back in Sept '03 was 27 seconds.

2. When asked how you would like to format your hard drive, choose ‘Format the partition using the NTFS file system’  
   There are conditions under which you may want to choose FAT32 instead. If you have a Windows 95/98/ME machine which will need to access files stored on this XP machine, or you are dual-booting with Linux, then you will need to have at least one FAT32 partition. In general, though, NTFS is a better and more secure choice than FAT32.
   Footnote FAQ #1: What is the difference between a regular format and a quick format?

3. Type in a strong Administrator password if (when) queried for it.  
   In no event should you use a blank password or a ‘generic’ password such as ‘administrator’, ‘password’, etc. Many current worms will attempt to guess passwords on mapped drives, and of course will go through many generic passwords. A strong password is at least 8 characters long, has both letters and non-letter characters, and mixed upper and lower case, preferably something that’ll mean something to you (ie, TG2reBxp0).
   Footnote FAQ #2: I don’t have anything private on my computer/account, why should I worry about my password?

4. Since your network cable is unplugged, just accept the default networking info.  
   Unless you know that you are part of a domain, just select being part of a workgroup.

5. When prompted, select LAN, then (most likely) DHCP (Obtain IP automatically) and obtain DNS automatically.  
   If you have a static IP, you should enter the information from Step 6 of the check list here

6. When asked to input usernames, just input one for now.  
   It’s easier to add more later than to add them now, since it doesn’t prompt you for any password if you make them now, and it’s easier just to make the entire account later after you have the proper security settings set up.

7. At this point, you should be past all of the initial configuration windows, and have the default (and insecure!) installation of Windows XP.  
   If you prefer other graphical settings than the default, go ahead and change them at the end of the guide since all the screenshots are taken with the default screens.
I. Rebuilding and Securing XP *[Critical]*
*(All new rebuilds should go through these steps)*

8. Put passwords on user accounts

*Click on Start->Control Panel->User Accounts, double click on your user account, and click on ‘Create a password’. Be sure to choose a strong password, and be sure to have a password for every account on your computer.*

_Footnote FAQ #2: I don’t have anything private on my computer/account, why should I worry about my password?_

9. Disable DCOM by following the screenshots

*If you need DCOM, you’ll likely know it.*

_Footnote FAQ #3: What is DCOM used for?_

a. Click on Start->Run, and type in: dcomcnfg

b. Double-click on "Component Services", then double-click on "Computers". Right-click on "My Computer" and choose "Properties".

c. Choose the "Default Properties" tab and uncheck "Enable Distributed COM on this computer". It should then look like the screenshot below. Click “Apply”, then "OK" and close the “Component Services“ (dcomcnfg) window.

d. Reboot your computer.
I. Rebuilding and Securing XP*Critical*
(All new rebuilds should go through these steps)

10. Install Symantec AV from CD

   Choose ‘Install Client’, and ‘Unmanaged’, unless you know you are specifically supposed to do otherwise

11. Run the Intelligent Updater from CD

   This is from the additional CD which you burnt for yourself, or which the Help Desk gave you. These are crucial virus definition files which have been added since Symantec AV was first released – if you don’t do this step, Symantec will not be able to catch most viruses and worms.

12. Schedule automatic Live Updates

   Click on the little golden shield icon on the lower right hand corner of the screen. You should see the below screenshot. Check to make sure that the date after ‘Version: ‘ is no later than the previous Wednesday (although it should probably be the date that you downloaded the Updater). While we’re here, we might as well schedule future updates to happen automatically on a daily basis. Choose a time where you think that your machine will be online daily, and preferably when you won’t be particularly busy working on it.

13. Be sure you have realtime protection enabled

   Check by going to Configure->File System Real Time Protection, and make sure the box marked ‘Enable file system realtime protection is checked.

14. Schedule regular Symantec scans

   Make sure that you only select your local hard drive(s) (most likely just the C: drive). A weekly scan should be sufficient (feel free to modify to either a daily or monthly) – pick a time when your computer will be on, but you won’t be using it extensively. This should not be the same time as when you download your updates.
I. Rebuilding and Securing XP *Critical*
(All new rebuilds should go through these steps)

15. Configure your network connection without the network cable plugged in
   Yes, your network cable should still be unplugged at this point. It’s possible that Windows XP may already have a network configuration correctly set up for you, especially if you use DHCP, but you should still go through and check.
   Start->Control Panel->Network and Internet Connections->Network Connections (lower right hand area)

16. Turn off bridging
   You may have bridging set up by default, such as for Firewire. This may cause the network port you are connected to automatically disable itself, depending on which building you are in.

17. Turn off Windows File and Printer Sharing (optional)
   Right click on your network connection(s), select Properties. You should be on the ‘General’ tab – uncheck the ‘File and Printer Sharing…’ box, then continue to the next step to turn on your firewall.
   Footnote FAQ #4: What does disabling File and Printer Sharing do? I map other network drives such as Occupant, should I still disable this option?

18. Turn on ICF for your network connections
   Right click on your network connection(s), select Properties (if you didn’t already do so from the previous step). Select the ‘Advanced’ tab, check the ‘Protect my computer…’ box, then click ‘OK’. Your machine may freeze momentarily when you first turn on the firewall. You may want to get a different firewall later, but having ICF on in the meantime is better than nothing.
   If you want to look into free firewalls available for personal use, you can check some of the references in Appendix B.
I. Rebuilding and Securing XP *Critical*  
(All new rebuilds should go through these steps)

19. Plug your network cable in, and reboot your computer  
Your computer is still insecure, but you’ll need to get on the network to get the latest Windows patches. Patching your computer regularly is crucial, since new bugs and exploits are found regularly and fixed by new patches.

20. Go to Windows Update  
(http://windowsupdate.microsoft.com)  
and install at least all critical patches  
Click on ‘Scan for Updates’. If asked prompted with a security warning, select ‘Always trust contents from Microsoft Corporation’ and click ‘Yes’.

You should end up with well over a dozen critical updates (this may change once SP2 or later comes out, of course). Please note that this process may entail several reboots.

Be sure to install all of the critical updates – go back to http://windowsupdate.microsoft.com after each reboot while you’re patching until there aren’t any more critical updates. After finishing with the critical updates, check through the ‘Windows XP’ and ‘Driver Updates’ sections to see if there are any other updates you want installed (sometimes patches which probably should be ‘critical updates’ are put in the ‘Windows XP’ category instead).

21. Set Windows Update to auto-update  
Left click on the Start button, right click on ‘My Computer’, and select ‘Properties’. Select the ‘Automatic Updates’ tab, and make sure that the ‘Keep my computer...’ box is checked. Select the Download Setting which you would prefer. Click ‘Apply’, then ‘OK’. Please note that if you choose one of the first two settings, you will have to remember to manually install the updates when an icon appears and reminds you that ‘New Updates Are Ready to Install’.

You may wish to note that the icon which appears to remind you that there are new updates only appears if you are logged on with administrator privileges. This is discussed in the below question.  
Footnote FAQ #5: Which download/installation choice do you suggest for Windows Automatic Update?
I. Rebuilding and Securing XP*Critical*
(All new rebuilds should go through these steps)

22. Revealing hidden files and extensions
Click on Start->My Computer, then on Tools->Folder Options. Go to the ‘View’ tab, and unselect ‘Automatically search for network folders and printers’, select ‘Show hidden files and folders’, unselect ‘Hide extensions for known file types’, ‘Hide protected operating system files’, and ‘Use simple file sharing’, then click ‘Apply’, and ‘OK’.

23. Set Internet Explorer to at least Medium Security
Start Internet Explorer (Start->Internet Explorer), and select Tools->Internet Options. Select the ‘Security’ Tab, and be sure that the ‘Security Level’ of the ‘Internet’ zone is set to at least ‘Medium’. Click ‘Apply’, and ‘OK’.
II. Additional Security Measures

Instructions and screenshots for these steps will be up in a few hours. Please check back. In the meantime, here is a list of other suggested steps for hardening your Windows XP system:

Turn off unnecessary services
• Change policies and audits
• Account Policies/Password Policies:
• Account Policies/Account Lockout Policy
• Local Policies/Audit Policy
• Local Policies/User Rights Assignment
• Local Policies/Security Options
• Network security: LAN Manger authentication level
• Importing a security template will take care of some or all of these:
• Password policies, account lockouts, audit policy, LMhash, NTLM2, access computer from network, change system time, log on locally, clear virtual memory, SAM accounts, force ctrl-alt-del
• Make an user account which will be your primary user account, with less than admin privs. Change your admin password, now that you have your policies set.
• Secure passwords, especially making sure that the admin password is secure
• Register your MAC address for a faster response if your secured system turns out to be insecure (http://www.its.caltech.edu/cgi-bin/macregistry.pl)
• Change the settings so you can see file extensions and hidden files. This is a lot more important than it used to be, now that many viruses use ‘double extensions’ (ie, hi.txt.exe to make an executable look like a text file).
• Turn off NetBIOS
• Password protect your BIOS
• Run the MS Baseline security analyzer
• Look into getting a firewall other than ICF
• Set Start Menu Security