Patching a Windows XP Install

January 2005

This document will go over some basic steps required to patch a Windows XP installation (XP Professional, Version 2002, Service Pack 2, v.2082) once you have installed. A list of steps, data required, reboots, etc. The same order of steps applies to other versions of Windows as well.

Minimum Required Steps

- After inital install download either the Mozilla Web Browser for Firefox from http://www.mozilla.org/ and use these browsers instead of Internet Explorer.
- Download all Microsoft Critical patches for Windows XP and apply them - including Service Pack 2 if your build of Windows XP does not include this.
- Turn on Windows built-in firewall or install third party firewall software.
- Turn off all unnecessary services.
- Install anti-viral software (Norton AntiVirus is recommended), and scan for viruses.
- Install anti-spyware/malware program(s). You can combine free versions of AdAware and Spybot fairly effectively, but the paid-for version of AdAware is a better way to go.
- Scan for spyware and malware. You may have become infected, particularly if you used Internet Explorer to view other pages before downloading Mozilla or Firefox.
- Be sure that all your software is automatically updating, or, at least, warning you when updates are available. This includes:
  Windows Update
  Antiviral software
  Firewall software (if third party)
  Anti-spyware/malware software

In addition you may need to download software to fully support the hardware you are using.

Step-by-step record of what was required to completel the above list

Windows Updates

1. The initial boot of Windows XP includes a new wizard that will ask you if you with to Turn on Automatic Update now: Say Yes to this!
   - If no network is found, then once you have started Windows you will need to go in to the Windows Update option under the Start menu ==> All Programs ==>Windows Update and begin downloading items.
   - If you install Mozilla Firefox (1.0) or the Mozilla (1.7.5) web browser and go to the Microsoft Windows Update web site this will not work as Windows Update *requires* that you use Internet Explorer version 5, or above. This is an issue as many of the security issues in Windows are directly related to using Internet Explorer.
2. Initial boot - You will be asked if you wish to turn on the Windows firewall option. If you are not using third party firewall software, then click the "Recommendations" button and click "Enable now" in the popup window that appears.
   - If no network connection is available as of yet turning on the firewall may fail, but there will be no indication that this failed because you don't have a network connection.
   - If you use an "open" (insecured) wireless network and you have a wireless card Windows XP will not enable your wireless connection by default. You must choose to connect to the insecure wireless network manually to use this connection.
   - In the Security Center Control Panel you may see an indication that the Firewall is off, but if you go to Control Panel ==> Network and Internet Connections ==> Windows Firewall you may find that this indicates that your firewall is turned on and functioning properly.
3. Once your computer has booted and you have a network connection, then you can run Windows Update (Start Menu ==> All Program ==> Windows Update). This will open Internet Explorer to the Windows Update page and an automatic check of your computer will be made to look for all available updates.
   - You may find that, by default, Internet Explorer automatically stops Microsoft from installing software on your computer. You will see a small message just below the Address bar in Internet Explorer telling you of this and asking you to "Click here for more options...". If you miss this, then eventually you will receive an error message in the Windows Update page itself with links to looking for help.
   -
   - If you click on the "Click here for more options..." text a popup will allow you to choose to "Allow this page to install ActiveX controls". Choose this, the page will reload, and then you'll be asked to install some software for Windows Update.
4. At this point you are asked to install a new version of Windows Update. Click on the "Install Now" button in your Internet Explorer window.
5. Software is installed automatically. No indication of actual size of installed software is given. It appears to be several hundred Kb in size.
6. Now you are asked if you wish to use Express Install or Custom Install. Express Install of updates is recommend. For purposes of this document we chose Custom Install.
7. Upon clicking on the Custom Install option Windows Updates scans for available udpates for your computer.
8. During the scan your browser window and animated cursor may freeze for some period of time. In the case of my machine Internet Explorer hung and I had to restart it.
9. Upon closing IE a new Windows Update icon was placed in the Start Menu. This icon directed IE to http://v5.windowsupdate.microsoft.com/, which did not respond. Upon opening the original Windows Update icon (Start ==> All Programs == Windows Upate) IE was directed to http://v5.windowsupdate.microsoft.com/v5consumer/default.aspx?ln=en-us.
10. IE opened at the page asking if I wanted to do the recommend Express Install or Custom Install. I clicked on Custom Install again.
11. At this point another error was displayed (Err number: 0x800706F7). I closed IE and restarted IE by itself.
12. I verified that network was functioning by going to http://www.msn.com/ and http://www.cnn.com/. I then manually went to http://www.microsoft.com/ and clicked on the Windows Update link. This link failed to display properly on the first try. I did a force reload, at which point I was redirect to the Custom and Express Install pages, which failed again.
13. At this point I checked the Internet Options Control Panel and verified that IE security options seemed reasonable (ActiveX controls allowed).
14. I rebooted Windows to see if this might help... The ol' standbye.
15. Upon reboot Windows XP hung with no output indicating why.
16. I tried booting again. This time Windows XP booted properly with no error messages.
17. Upon rebooting the Security Center correctly noted that my Windows firewall software was enabled.
18. As an aside, Microsoft Instant Messenger started and minimized on its own.
19. I ran Windows Update again, this time from the initial icon (who's position had moved in the Start Menu again) in the Start menu.
20. I was directed to the Express and Custom Install windows again. I chose Custom Install.
21. This time I was presented with a list of 5 possible updates totalling 2.1MB. These items were:
    - Security Update for Windows XP (KB87339)
    - Security Update for Windows XP (KB885835)
    - Critical Update for Windows XP (KB886185
    - Security Update for Windows XP (KB885836)
    - Microsoft Corporation - Sound - Crystal SoundFusion(tm) WDM Interface

    Only the initial update included any form of description in the Window. If you understand the Microsoft Knowledgebase you can use the KB numbers to find the articles pertaining to each update.

22. I clicked on "Go to install updates...
23. The same page was displayed again except the "Go to install udpates..." button had changed to "Install..." I clicked this button.
24. A status window appeared:
    - The Crystal SoundFusion update was downloaded.
    - Next two security updates, then the critical udpate, then security udpate were downloaded.
    - The Crystal SoundFusion update was installed (3 updates actually).
    - The two security updates, then critical update, then security update were installed.
25. Upon successful install I was asked to restart the computer. I clicked on the "Restart Now" button.

Next Steps

Once you finish with Windows Update then you need to take the following steps:

1. Turn off unnecessary services. This is a bit tricky with Windows as so many services are interconnected in upexpected ways. But, for instance, if any web, ftp , messenger services are running that you are not using, then turn these off.
2. Turn off Universal Plug and Play and the SSDP Discovery Service. If you are firewalled this is not as critical. To do this do the following:
    - Go to Control Panel ==> Performance and Maintenance ==> Administrative Tools.
    - Disable UPnP Device Host by double-clicking on the service and selecting "Disabled" in the drop-down menu.
    - Next go to the SSDP Discovery Service, double-click and select to stop the service.
    - Once stopped disable the service permanently by selecting "Disabled" in the drop-down menu.
3. Install antiviral software. Your choice, but Norton Antivirus is an excellent program and allows for automatic updating of its files in an easy and smart manner.
4. After/during antiviral software install scan your entire drive for viruses.
5. Install anti-spyware/malware software. Either purchase the professional version of AdAware, or install both the free versions of AdAdware and Spybot. You will need to manually update the defintion files for these products and manually scan for spyware/malware that is installed. you can setup spybot to automatically scan upon reboots, but it is not all that elegant and does not capture all of the spyware/malware infections you may run across.
6. Make sure you are using good passwords. Many people leave their administrator and user passwords blank or trivial to guess. Several security exploits take advantage of this fact. Be sure to use real and strong passwords for your Windows accounts.

The Conundrum for the End User

As you can see this whole process can become rather complex. This is something that an experienced user can do with relative ease, but a new user might get confused or lost. Compared to Windows 2000 the Windows Update process has improved (in spite of the glitches reported here), and the built-in security features as well. But, there are still several critical issues confronting end-users of Windows systems that do not have easy solutions. These include:

- Currently there doesn't appear to be a robust and easy to install free antiviral program for Windows.
- Spyware and Malware have now become as destructive as viruses. Currently there does not appear to be a robust, free and easy to use anti-Spyware/Malware program available for Windows.
- By default Windows includes Internet Explorer and Outlook. Both these programs contain numerous security holes. Getting users to switch can be hard, but not impossible. You have options (Firefox/Mozilla/Opera for web browsing, Thunderbird and many others for email).
- For users on slow connections downloading udpates to windows, viral software, and anti-spyware/malware software may be next to impossible. For instance, downloading Service Pack 2 on a 56Kbps modem connect was not really a viable alternative for most end-users.

So, while it is possible to make your client Windows install fairly secure, it is not easy. Some organizations provide security CDs that automatically check a client's computer and installs all the needed updates. The University of Oregon is one such group. You can read about their Security CD for Windows here.

A major issue for clients that do not have money or access to fast enough downloads is paying for software. To properly protect a Windows installation it is *absolutely essential* that each user run good antiviral software that is kept up-to-date and good anti-spyware/malware software that is kept up-to-date. If either of these items are not installed, then the client will almost certainly experience some form of infection via a virus, spyware or malware, possibly in a very short period of time.

Hervey Allen
Last modified: Sat Jan 1 13:22:29 CLST 2005