Global Information Assurance Certification Paper

Securing the new Windows XP

Karl G Johnson
MBUS 511 SANS Security Essentials
GSEC Practical Assignment Version 1.2f
November 23, 2001

Introduction

I have been working with Windows since version 3.1 and watched it evolve from its rudimentary beginnings. Now, for the first time, all the separate platforms of Windows 95, 98, ME, NT and 2000 are now being converged into a single operating system eXPperience, according to Microsoft, which they have baptized Windows XP.

Some experts say Windows XP is the best of its breed, improving on lessons learned from its predecessors Windows NT and 2000. Others say it is the beginning of a new doomsday device for hackers, which will promote "zombie code" throughout the Internet. From my recent research and short experience with XP, since its beta release over a year ago, each of these scenarios could play out depending on your point of view and how much effort is placed on implementing its security inheritance from Windows 2000 with its new enhancements.

So far, according to reports from security analysts and privacy advocates, testers have not been able to find any serious security threats in XP (except for several potential vulnerabilities brought to attention during beta months). According to John Pescatore, Senior Security Analyst at Gartner, Inc., "with Windows XP, Microsoft has at least fixed the sins of their past, which is more than I can say for other operating systems." These same analysts, advocates and testers have also praised Microsoft for taking care of the security atrocities that have haunted them from the Windows 9x and NT days. It's their opinion that the new security enhancements such as the embedded firewall, new authentication provisions and software restriction policies will do much good in protecting home users, especially those vulnerable to Cable or DSL lines to the Internet.

However, on the other face of the coin, there are those experts which still think that Microsoft doesn't have security as a top concern on their priority list, not more than just a list of features. This mindset revolves around, among other things, its inclusion of the Indexing Service {a later version of the software that was exploited by the Code Red Worm) and a fundamental change in the Windows XP security model involving Raw Sockets.

My intention here is not to praise or deface Windows XP, it is to bring into light, some of its security attributes worth considering, current security concerns and some configuration tips in how to make the best of your Windows eXPerience a secure one.

The XP Security Model

XP's security model is based on Windows 2000 with some distinctions between the Home and Professional versions and a few new enhancements. Most of the new security enhancements revolve around the Internet Connection Firewall, Password/Authentication

features and new Local Security policies. According to Mark Croft, Lead Product Manager for Windows XP at Microsoft, "the fundamental architecture of the operating system has also been "hardened," or made more secure."

Inherited from Windows 2000, XP uses a more robust NT File System than that of its predecessor old Windows file system. The Access Control Lists on system files and directories are more secure than was the case with Windows NT. In fact, NT ACLs where setup in a way that allowed regular users great leeway in installing software, which equally permits installing malware such as Trojans. Windows XP, by default, restricts the installation of system files to the Local System and Administrators Group.

One fundamental change in Windows XP that has caused pandemonium across some security experts and other advocates is its implementation of Raw Sockets. This issue was brought to the attention of Microsoft and the industry by Steve Gibson from Gibson Research Corporation, developer of the SpinRite disk utility and author of a free Windows security test known as Shields Up. Gibson claims that Microsoft's approach in opening UNIX style Raw Sockets in Windows XP to provide additional security functionality, such as the Internet Connection Firewall, will create a "backdoor" that will provide full and direct "packet level" Internet access to any UNIX sockets programmer. He understands that this, in addition to the huge number of projected XP installations worldwide, will motivate hackers to find new ways to penetrate XP systems and create an undetectable army of "cable bots" running "zombie code" to propagate DDoS attacks. They will be undetectable, because the Internet Connection Firewall will make these systems invisible in the Internet.

So the dilemma seems to be improving security with new enhancements by implementing Raw Sockets to protect you from hackers coming in or sacrifice perimeter security to fight hackers once they get in. In my opinion no operating system is 100% secure, which means there is always the probability of compromise, but the first line of defense should be keeping anyone from coming in and then being able to deal with it if they do get in. The new security implementations that are sacrificed by opening Raw Sockets will make it harder for hackers to get in than ever before. Combine this with other security features such as Software Restriction Policies, Anti-Virus software, Service Packs and Security updates and we could have the most secure Windows OS to date. As a rule in favor of Gibson's concerns, Microsoft should redesign XP's new security enhancements to limit their access to Raw Sockets only to the System Level account or Administrators Group, much in the same way that other operating systems, such as UNIX, limit this access to "root" level privileges. Although, once the attacker has control of the machine they could be able to add Raw Socket level functionality by modifying any standard OS systems files through some type of third party device driver.

New Security Features

XP's new security features will only be effective if they are enabled and configured properly. Some of these features will be enabled by default others need attention. In some features their behavior will change depending if it is the XP Home or Professional Edition and whether it is a standalone, member of a workgroup or, in case of Professional, a domain. Among these features are improved authentication, a Credential Manager, file encryption, Internet Connection Firewall, Remote Desktop and new software restrictions.

Authentication

Authentication has definitely improved more for the Home Edition user than for the Professional, since now you must login in order to access the system, unlike its Windows 95, 98 and ME predecessors. The only drawback is that in a standalone installation XP will allow you to choose a blank password. This is where the Blank Password Restriction feature comes into play, by limiting you to only login locally at the console and not remotely. Additionally you cannot use the secondary logon service (RunAs) to start a program as another local user with a blank password. In either case, it is good practice to assign a strong password to on all local or domain user accounts to prevent any chance of a compromise.

Under Programs > Administrative Tools >Local Security Settings using Classic Mode or Control Panel > Performance and Maintenance > Administrative Tools > Local Security Settings you will find the policies that control authentication features such as passwords, expirations, history, etc. By default in XP the Account Lockout Threshold is set to 10 invalid logon attempts and Maximum Password Age is set to expire after 42 days, otherwise all other settings are set to zero or not enabled. XP's policy option of using *reversible encryption for storing passwords* **should not** be enabled since passwords are typically stored as hashes and the value based on the password is not reversible. To configure your password and account policies, start by going through all the policies under Account Policies and set these recommended values:

Password Policies
- Enforce password history: 10
- Maximum password age: 60
- Minimum password age: 10
- Minimum password length: 8

Password must meet complexity requirements: Enabled

Account Lockout Policy

Account lockout duration: 1 hour

Account lockout threshold: 3 invalid logon attempts

Reset account lockout counter after: 1 hour

Passwords are your first line of defense, configure your Account Policies wisely and they will go a long way towards securing your XP system.

Additional policies that have an effect in authentication or access are defined below and you should considering applying them to further secure your system (make sure your account belongs to one of the groups that remain when removing the Everyone Group):

User Rights Assignment

Access this computer from the network: Remove the Everyone Group

Bypass traverse checking: Remove the Everyone Group

Security options

Accounts: Rename administrator account: Enter a different user name for Administrator

Accounts: Rename guest account: Enter a different user name for Guest

Interactive logon: Do not display last user name: Enabled

Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enable

Shutdown: Clear virtual memory pagefile: Enabled

An authentication alternative available with XP is the use of Smart Cards. Windows 2000 provided you with the ability of login on with smart cards. Windows XP has enhanced on its functionality to utilize smart cards on Terminal Servers and to run administrative tools and utilities. One drawback to this technology is that keystroke monitors can collect your smart card PIN, but the attacker will still need the card to make any use of this information. Another drawback to watch out for is to hibernate your system instead of shutting it down. In doing so anyone who powers on your system will have access up to the point where you left off before hibernating. When using smart cards please make sure to apply the **Interactive logon: Smart card removal behavior: Lock Workstation** setting under Local Policies > Security Options so your workstation is locked when the smart card is removed, allowing you to leave the area, take your smart card, and still maintain a protected session.

Credential Manager

The Credential Manager consists of three main components: credential prompting user

interface, stored user names and passwords and the keyring. By combining these elements XP creates what they called a single sign-on solution. The user interface will prompt you with a "remember password" option to save your credentials to the Stored User Names and Passwords roamable store. The only catch is that only integrated authentication packages will be saved (such as Kerberos, NTLM, SSL, etc.). When you access a resource through an integrated authentication package and the credential is found in the store, it will be used automatically without any user intervention. Only an integrated authentication package can retrieve credentials from the store. The keyring is the component that will allow you to manually manage your credentials in the store through the User Accounts Control Panel applet under Manage Passwords in the Advanced Tab. The availability to save your credentials in the store is controlled by a Group Policy in the Local Security Settings Console under **Local Policies** in **Security Options** called ***Network access: Do not allow Stored User Names and Passwords to save passwords or credentials for domain authentication***. XP by default installs it in a disabled state which allows the storing passwords and credentials. There is also a credentials prompting API for developers in the Platform Software Development Kit to incorporate this mechanism into their applications when required.

File Encryption

File encryption is an inheritance from the Windows 2000 platform. XP has improved upon it enabling it by default, adding encryption support for cached files, allowing multiple users to access an encrypted document and supporting file sharing with Web Developing Authoring and Versioning (WebDAV). Encryption is automatic to the user without any intervention and appearing in green to distinguish them from other files, while still controlling their state through Windows Explorer on a file or folder basis. The addition of cached file support is a good idea for those who travel, preventing unauthorized access to offline files in case your notebook is lost or stolen. WebDAV support will allow you to use HTTP to access files remotely, even through firewalls, by keeping files encrypted while transmitting them through public access. I will have to admit that this practice of tunneling through firewalls to move files offsite will require a lot of faith on the part of security managers in order to be widely adopted in corporate environments.

A few things to be aware is that encryption is only available on an NTFS volume. If you are using FAT or FAT32 you must convert your file system to NTFS. To accomplish this go to Start > All Programs > Accessories > Command Prompt. At the command prompt enter **convert c: /fs:ntfs**, replace the c drive with the appropriate drive letter. For further information on this process go to the following link: HOW TO Convert a FAT16 or FAT32 Volume to NTFS. So far the only flaw is that if your folder view is set to Thumbnail, the contents of the file may still be visible while encrypted. More information on this condition at the following link: You Can View an NTFS Encrypted

File in Thumbnail View.

Please take the time and review these other links relevant to XP and EFS:

- Best Practices for Encrypting File System (Q223316)
- HOW TO: Back Up Your Encrypting File System Private Key (Q241201)
- "Access Is Denied" Error Message Appears When Permissions Are Correct (Q250494)
- Encrypted Files Made Available Offline Are Not Encrypted on the Client (Q254156)
- Registry Keys Used to Tune EFS Caching (Q278256)
- Enrollment Does Not Succeed on Windows XP When Requesting a Certificate by Using a DSS CSP (Q300860)
- HOW TO: Encrypt a File in Windows XP (Q307877)
- HOW TO: Encrypt a Folder in Windows XP (Q308989)
- HOW TO: Share Access to an Encrypted File (Q308991)
- HOW TO: Remove File Encryption in Windows XP (Q308993)

Internet Connection Firewall

One of the most talked security features in Windows XP is the new Internet Connection Firewall (ICF), which is enabled by default when using the networking wizard. It is a stateful based firewall that filters inbound packets without regard for outgoing traffic. As John Pestatore puts it ICF offers "rudimentary blocking," only ideal for those home, SOHO or small business users that have high-speed cable or DSL connections to the Internet. In the corporate world, it could also be useful for remote access and telecommuters.

The concern with ICF is that it only stops hostile or other inbound traffic and is indifferent to outbound traffic. Here is where the danger lurks with code such as viruses, Trojans or adware trying to access the Internet without permission. Nevertheless, to test its effectiveness some individuals ran a series of common scans using the nmap UNIX tool against XP with ICF enabled. The results provided where interesting. On the TCP connect (nmap –sT) and TCP SYN (nmap –sS) scans ICF returned nothing, displaying that there was no host address specified. I also tested ICF using Gibson's Shields UP, which reported that the system was running in "full stealth mode" its more secure rating. This means that when ICF is enabled your system is virtually invisible to those lurking on the Internet. Although I don't underestimate the ability of hackers to find a way around ICF, it is a big improvement from what Windows had in the past. This will make it harder for hackers to install malware for converting systems into distribution nodes to propagate their malicious code as long as they don't get in through a "backdoor."

For users connected to a corporate or private internetwork, ICF could constrain your networking capabilities. Network services such as email, FTP, NetBIOS file sharing, RPC

(required by Outlook and Exchange), VPNs and other services can be affected. In these of environments is it a good idea to not use ICF and to provide defenses with a company Proxy or firewall. In some extreme cases you could still enable some of these services through ICF from the Settings section in the Advanced tab on the network connection properties dialog. In order for system administrators to avoid any of these issues, Group Policies could be implemented that can prevent users from enabling ICF while connected to the corporate network.

Those of you interested in not using ICF and installing some third party desktop level firewall, **please be absolutely sure** that it is compatible with XP. I speak from experience. I tried versions of Network Associates (McAfee) and BlackIce personal firewalls on an XP system and both resulted in Blue Screens. I had to run System Restore (thank God for this feature) in Safe Mode to backup to previous restore point in order to get the system running again.

Please take the time and review these other links relevant to XP and ICF:

HOW TO: Enable the Internet Connection Firewall Feature in Windows XP (Q283673)
Service Redirection Does Not Apply to Internet Connection Firewall (Q297942)
The Internet Connection Firewall Can Prevent Browsing and File Sharing (Q298804)
Internet Connection Firewall Does Not Block Internet Protocol Version 6 Traffic (Q306203)
Troubleshooting Internet Connection Sharing in Windows XP (Q308006)
Troubleshooting Home Networking in Windows XP (Q308007)
Internet Programs May Not Work as Expected with the Internet Connection Firewall Enabled (Q308123)
How to Manually Open Ports in Internet Connection Firewall in Windows XP (Q308127)
Norton Personal Firewall 2.5 and Internet Security 3.0 Do Not Work in Windows XP (Q308324)
Creating a Bridge with Two Internal Adapters on a Windows XP Internet Connection Sharing Host Does Not Work (Q309640)

Remote Desktop/Assistance

Remote Desktop and Remote Assistance are new additions in XP not considered to be security features, but they definitely could be exploited as an avenue to compromise the system. There is concern among experts on these features since they are based on the Windows Terminal Server code of which there have been 251 vulnerabilities listed on the CERT Web Site alone.

According to reports if your system is using a continuous service like cable or DSL there can be a risk with these terminal based services. On XP using the Remote Desktop, any

member of the Administrators Group can connect using the Terminal Services client. If you don't rename the Administrator account, as suggested previously, and use a weak password a hacker can easily have access to your system with typical password cracking software and it will be Game Over. For systems under cable or DSL connections that are always online I recommend that you turn these features off unless you can turn them on for a support issue then turn them off again. It is not advisable to leave them on all the time. Although Microsoft has placed some checks and balances to prevent a compromise with these features it is better to be safe than sorry. If you still require to use these services it can be advantageous to use a different port other than the defaults. To implement this follow the instructions on these links: Configuring the Remote Desktop Client to Connect to a Specific Port (Q304304) and How to Change the Listening Port for Remote Desktop (Q306759. System administrators can disable this feature using Group Policies following the instructions on this link: How to Disable Remote Desktop by Using Group Policy (Q306300).

Software Restrictions

The last line of defense in the new XP security model is the ability to restrict code from running using the Software Restriction Policies. One of Microsoft's defenses from Gibson's Raw Sockets allegations is that with Software Restriction Policies, we can prevent malware from running if our system is compromised. These Software Restriction Policies consists of enforcement rules, designated file types, trusted publishers, security levels and additional rules. I have to admit that these policies are cleverer than previous attempts, with the capability of using hashes that can work even if application in renamed. Although, it is possible that someone can disrupt the hash algorithms by using a binary editor by tweaking a few bits, in this case using digital signatures can do the trick. You can set rules based on digital signatures/certificates, hashes, Internet zones or directory paths. These policies will be particularly good against unsuspected email attachments carrying malicious code that would otherwise not get in through the front door.

By default Software Restriction Policy install as "Unrestricted" which means that software access rights are determined by the access rights of the user. The more secure approach is to set it to "Disallowed" which means that software will not run, regardless of the access rights of the user. Since setting up these policies is a detailed and intrinsic process I doubt that the average novice user will bother or have the necessary knowledge to implement them. They do provide a great tool for defense if you know how to use them and apply them properly, like for example in a corporate setting, where they can be applied through GPOs. For more detail information on these policies go the following link on Microsoft TechNet.

Final recommendations

My final recommendation in securing your Windows XP system is to follow these configuration recommendations:

- ✓ Verify that all your disk partitions are formatted with NTFS
- ✓ Protect all file shares, for XP Home Edition use the "Make Private" feature
- ✓ For home, small business or SOHO users use Internet Connection Sharing for shared Internet connections
- ✓ For home, small business or SOHO users enable the Internet Connection Firewall
- ✓ Use and enforce strong passwords
- ✓ Install anti-virus software and updates
- ✓ Keep up-to-date on the latest security updates by configuring Auto Update (System in Control Panel selecting Automatic Updates)
- ✓ Disable unnecessary services
- ✓ Disable or delete unnecessary accounts
- ✓ Make sure the Guest account is disabled
- ✓ Rename your Administrator Account
- ✓ Disable or change default ports on Remote Desktop service
- ✓ Set stronger password and account lockout policies as suggested previously
- ✓ For Outlook 2000 users install the Email Security Update, to prevent email attachments from being launched
- ✓ Set Software Restriction Policies

I have to admit that Microsoft has taken serious steps on improving security at the desktop, but there is still much more that can be done. The difference now is that there is a glimpse of light at the end of the dark cyberspace tunnel. Only time will tell if unprivileged raw sockets access or any of the security features in XP will turn out to be benign or disappointments.

References

Books

Minasi, Mark. "Mastering Windows XP Professional." September 2001. ISBN: 0-7821-2981-1

Magazine Publications

Rash, Wayne. "Next Up: WinXP… And More Headaches." October 22, 2001. InternetWeek.

Radcliff, Deborah. "Windows XP: Is it safe?" October 22, 2002. Computerworld.

Online

Fontana, John. "Former Fed Says XP Poses a Security Threat." October 15, 2001. Network World. URL: http://www.pcworld.com/news/article/0,aid,66023,00.asp (November 2, 2001)

Mullen, Tim. "Did too many cooks spoil Windows XP Security?" September 15, 2001. Security Focus. URL: http://www.securityfocus.com/columnists/24 (November 24, 2001)

Livingston, Brian. "Windows XP and DDoS." June 11, 2001. devX. URL: http://gethelp.devx.com/pubs/infoworld/vol23/issue24/010611oplivingston.asp (September 1, 2001)

Mc Williams, Brian. "Windows XP: A Hacker's Dream?" June 7, 2001. Newsbytes. URL: http://www.newsbytes.com/cgi-bin/udt/im.display.printable?client.id=newsbytes&story.id=166598 (September 10, 2001)

Greene, Thomas C. "MS security chief talks raw sockets with the Reg." July 13, 2001. The Register. URL: http://www.theregister.co.uk/content/4/20387.html (November 7, 2001)

Gibson, Steve. "Why Windows XP will be the Denial of Service Exploitation Tool of Choice for Internet Hackers Everywhere." July 19, 2001. Gibson Research Corporation. URL: http://grc.com/dos/winxp.htm (October 30, 2001)

Thurrott, Paul. "Is Windows XP Safe? A Look at a Growing Controversy." July 24, 2001. Windows 2000 Magazine Security Administrator. URL: http://www.secadministrator.com/Articles/Print.cfm?ArticleID=21906 (November 14, 2001)

Weigel, Ray. "Inside XP: Internet Connection Firewall." July 24, 2001. TechTV. URL: http://www.techtv.com/products/print/0,23102,3338448,00.html (November 15, 2001)

Swoyer, Stephen. "Review: Windows XP's Built-in Firewall." September 24, 2001. ENT News. URL: http://entmag.com/news/print.asp?EditorialsID=4963 (November 14, 2001)

Vamosi, Robert. "Windows XP just doesn't cut it in the security department." October 23, 2001. ZDNet. URL: http://www.zdnet.com/filters/printerfriendly/0,6061,2819732-2,00.html (November 7, 2001)

Williams, Jim. "Windows XP Security: Windows XP Internet Connection Firewall." July 16, 2001. About.com. URL: http://netsecurity.about.com/library/weekly/aa071601a.htm

(November 7, 2001)

Farrow, Rik. "Windows XP: Security by Complexity." October 5, 2001. Network Magazine. URL: http://www.networkmagazine.com/article/printableArticle?doc_id=NMG20011004S0009 (November 15, 2001)

Reuters. "Windows XP includes beefed-up security." October 24, 2001. ZDNet. URL: http://www.zdnet.com/filters/printerfriendly/0,6061,5098754-2,00.html (November 7, 2001)

Andress, Mandy. "How will Windows XP cope with security?" May 14, 2001. ITworld.com. URL: http://www.itworld.com/Comp/2218/IWD010514tcwindowsxp/pfindex.html (November 1, 2001)

Lee, Stephen. "RSA: Microsoft outlines .NET and XP privacy strategy." April 11, 2001. InfoWorld. URL: http://www.infoworld.com/articles/hn/xml/01/04/11/010411hnmsrsa.xml (November 1, 2001)

Technical Reference

Hostile Code, not the Windows XP Socket Implementation, is the Real Security Threat http://www.microsoft.com/technet/security/news/raw_sockets.asp?frame=true

What's New in Security for Windows XP Professional and Windows XP Home Edition http://www.microsoft.com/windowsxp/pro/techinfo/planning/security/whatsnew/default.asp