Global Information Assurance Certification Paper

An Analysis of Windows XP Service Pack 2: Does it Provide In-Depth Security for the Home User?

Julie Driscoll
December 9, 2004

GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4c – Option 1

Version 1.4.c

Abstract

Windows XP Service Pack 2, primarily a security enhancement upgrade, was released earlier this year. As a response to the continual increase in threats and vulnerabilities, Microsoft focused on improving XP's defenses against viruses, worms, and other malware. This paper provides an overview of the many changes in SP2 and whether or not they provide in-depth defense to the XP Home user. It's widely agreed that this service pack provides needed security improvements, and that users should upgrade their Windows XP systems. However, XP remains a complex system that requires IT skills beyond the average home user in order to remain secure.

Table of Contents

Introduction

Earlier this year, Microsoft released the long awaited and much publicized Windows XP Service Pack 2 (also referred to in this paper as XP Home or SP2). It is an update focused on enhancing security in order to improve XP's ability to "withstand malicious attacks, especially those from viruses and worms."[1] and it includes all patches up to August 2004 security releases. XP Home provides the least functionality of the XP family and is designed for the home user's stand-alone, desktop computer. This does not exempt it from security concerns. On the contrary, since it is not administered by IT professionals, it may be more vulnerable to attack. The focus of this paper will be a description of the enhancements of Windows XP Home SP2 and whether or not they provide the home user with in-depth computer security.

Microsoft has made significant improvements in providing in-depth security. However, many of the enhancements require assistance from highly skilled Network or IT administrators. The XP Security Guide and Test Guides provide a wealth of information on how to configure optimal settings through templates and group policies.[2] It details how administrators can define features such as account policies, including password complexity and expiration, auditing, event log settings, and rights and permissions for the workstations in their domains. The XP Security Guide Setting spreadsheet, contained in the Security Guide, contains more than 200 configuration options. Appendix A is a 231 page document that discusses specific changes to SP2. Does Microsoft provide similar configuration information for the stand-alone, home user? If so, how would a home user tackle its volume and complexity?

Microsoft's Security at Home website is a useful resource for the home user. There are hundreds of links discussing a variety of topics including preventing viruses, fighting spam and spyware, and safe online shopping. It provides links to security awareness sites such as Web Aware, GetNetWise, and the National Cyber Security Alliance.[3] The average home user can easily spend several hours reading about how to protect their PCs. However, Tom Greene, a writer for The Register, suggests that placing this burden on the average computer user is not the best approach. He asserts that Microsoft has not done an adequate job at protecting the home user. He writes, "The home user is the one most in need of good security configurations and tools, yet the one least served by SP2."[4]

Defense In Depth

SP2 is marketed as providing better security. Based on SANS security training materials, security essentials should at least include enforcing the following features: complex passwords, account lockout, principle of least privilege, encrypted file system, disabling services, internet firewall, backups, and maintenance.[5]. (There may be more security issues discussed, but they are not in the scope of this paper.) These security features, coupled with the 'Defense in Depth' paradigm should be the goal of safe computing. Defense in depth means

that multiple layers of protection are employed in each area of computer architecture. If one layer fails, another layer provides protection. And if all layers were to fail, "we need to be ready to detect that something has occurred and clean up the mess expeditiously and completely."[6]

Of the eight essential security features noted above, only one is enabled in the default configuration of SP2. The Windows Firewall is installed and enabled by default, however, it does not provide egress filtering.[7] More details about the Windows Firewall may be found in a later section. SP2 does disable some unnecessary services and the principle of least privilege is now a part of the DCOM and RPC services, but this principle is not integrated throughout the system. The principle of least privilege means not giving a user or process more control than necessary. XP Home users are automatically a member of the Administrators Group. This gives users more access than needed and if a hacker were to get access, she would then automatically have Administrative access. Furthermore, Windows XP Home does not enforce the use of passwords. Not using a password makes a hacker's job of 'owning' a PC very easy. There's no password complexity enforced and this makes cracking the password extremely trivial. Account lockout is a necessity to protect against multiple login attempts. Likewise, logging access attempts and failures is a useful way in detecting suspicious activity and providing forensic information.

XP Home does not offer a default file encryption capability and SP2 still does not offer it. If a home user stores their bank account information on their home computer, they have no built-in means of encrypting this important data. Likewise, a back-up utility, one way to recover from system crashes or compromises, is not installed in XP Home SP2 by default, but is available.

Disabling unnecessary services is a topic of debate in Windows XP. There are many dependencies in Windows services and venturing into the Services applet may be risky even for IT professionals.[8] The following services are now disabled with SP2: ClipBook, Alerter, Messenger, Network DDE, and Network DSDM.[9,10] However, some think that there are still many services that are not needed on a stand-alone system and should also be disabled. Examples are DHCP Client, DNS Client, NetMeeting Remote Desktop Sharing, Remote Assistance, file and printer sharing, Client for Microsoft Networks, QoS Packet Scheduling.[11]

As shown in the previous paragraphs, Windows XP SP2 does not address some basic security concerns. SP2 is 300+MB download. What does it provide then? Obvious changes are the Security Center, IE's pop-up blocker, and IE's Manage Add-Ons. Architectural changes, at the network and application layers, although transparent to the user, were a large part of SP2. These changes may prove to be essential security changes that mitigate buffer overflow and malicious code attacks. And it demonstrates that SP2 efforts are to provide a layered defense strategy. This is one kind of protection home users require. On the other hand, in the discussion that follows, it's evident that XP relies on the user's ability to make

good decisions about their own security. And most security professionals know that this is not always the best practice.

The following paragraphs discuss major enhancements available with SP2. However, changes implemented by group policy or templates are not discussed because these issues are generally handled by experienced administrators. Also, wireless technology changes, issues unrelated to security, and the addition of Bluetooth drivers and capabilities will not be discussed.

XP SP2 Enhancements

Windows Security Center

Windows Security Center is a new Control Panel applet that is installed with SP2. It is basically a pretty window that provides status alerts of the Windows Firewall, Automatic Updates, and Virus Protection. It gives the user a kind of dashboard view of the security status of their PC. Users can change options for the Firewall, Automatic Update and Internet Explorer using links in this window. The Security Center alerts the user with a status change using a red, green, or yellow light, reminiscent of Homeland Security Threat Advisory color coding. Some professionals believe that the Security Center provides a false sense of security.[12],[13] And, that providing the simple window will lead users to be less vigilant. Greene states that, "The Security Center is a good idea, but as it's been implemented, it's little more than a gimmick that will lead to a false sense of security."[14]

Windows Firewall.

Windows Firewall, an enhanced version of the Internet Connection Firewall, is ON (enabled) by default in SP2. It blocks incoming connections from the internet thereby creating a barrier between the XP desktop and the waves of traffic, some carrying malicious or intrusive code. Windows documentation notes that File and Printer Sharing and Files and Settings Transfer Wizard are defaulted exceptions in the firewall.[15] Remote Assistance was added to the exceptions and automatically allowing this is may be "a great boon to script kiddies"[16]. The new Windows Firewall also offers boot-time protection whereas ICF protection was dependent on various drivers starting before filtering began. While this firewall is an improvement, HP is replacing the Windows Security Center with Symantec's Norton Security Center on its new PCs. It contains all the features of Windows Security Center and provides a more robust firewall that blocks both inbound and outbound traffic and is packaged with anti-virus software as well as Windows Automatic Updates.[17]

Most home users would not know (or care to know) what a Firewall is or how to configure it without further research. After installing SP2 they are given information about configuring it and help links are provided. Users may also access Microsoft's Security at Home website. It provides a simple 1, 2, 3 approach to securing the PC. The first step is using an Internet Firewall. I selected the XP Operating System and clicked Next. The next page provided information on Windows Update. There was no description of what a firewall is or why it's important. Microsoft should include a link to a couple of knowledge base articles

on the Windows Firewall.[18]

But a major drawback to Windows Firewall is that it provides filtering on incoming packets only – no egress filtering[19]. Note that Microsoft recommends to continue using a third party firewall if you already have one installed.[20] Without filtering outbound traffic, there's no protection if a worm, virus, trojan, or spyware infect a user's PC and starts sending out traffic. Using a bidirectional firewall is a more secure option that provides an extra layer of defense.

Anti-Virus.

Virus Protection is not included in SP2, although it is essential in protecting users from email viruses, worms, trojans and other types of malware. The Security Centers displays a red OFF button when virus protection is missing and also shows a red shield in the system tray. It also lets users if their virus definitions are not up-to-date. Also, note that if you do not have a popular AntiVirus application, Windows may not recognize it.[21] To reduce compatibility problems and provide needed virus protection, home users may be better served to use a complete solution provided by Symantec's Norton Security Center, or a similar product.

Automatic Updates.

The Automatic Updates service provides updated software and is run at certain intervals and when critical patches are released. Automatic Update connects the PC to a Microsoft download site when updates or hotfixes are available, similar to the functionality of an Anti-Virus automatic update. The default time setting is 3am. If the PC is not powered on at that time, it will update the next time the power is on. More flexibility in changing this setting may be found in the Automatic Update link at the bottom of the Security Center Window, or under System>Automatic Updates.

Many people are opposed to allowing an outside connection without your immediate knowledge.[22] After all, isn't this one way computers get infected with malicious code? IT staff monitor updates and use tools such as SUS, and GPO to control content distribution. However, the home user may not be aware of updates, or the importance of applying them as soon as possible. The service is not turned on automatically, but users are given multiple warnings suggesting it be turned 'on'. An alternative to Automatic Updates is simply subscribing to Microsoft's Security Subscription Service. Users receive emails of important security updates.

Data Execution Prevention (Buffer Overflow Prevention)

Data Execution Prevention (DEP) or the "no-execute" feature marks certain memory locations and does not allow code execution on the marked locations. It prevents "code execution from data pages".[23] It's an enhancement that attempts to prevent buffer overflow attacks. Mark Minasi, a Windows expert, writes that DEP technology in "XP and 2000, would have stopped Code Red, Nimda, Nochia, Slammer, and Sasser cold, with no other patches installed. It's a good idea and a welcome addition to XP."[24] He also notes, however, that it likely slows

performance. Even so, this feature is not only a security improvement in the Windows OS, but it is done behind the scenes and without user intervention. This is the type of security enhancement that provides protection at the hardware and application layers and is needed for all users.

There are two types of DEP: hardware and software DEP implementation. Hardware DEP marks memory locations as non-executable, unless a program exists in that location.[25] Microsoft notes that both AMD and Intel are designing compatible "execution protection" microprocessors that make use of this new technology. However, David Berlind of ZDNet writes that most Intel systems don't support the feature, while AMD has been manufacturing DEP-enabled microprocessors for almost a year.[26] The software data execution prevention feature, claims to prevent some types of attacks and "helps protect only limited system binaries, regardless of the hardware-enforced DEP capabilities of the processor."[27] By default it is turned on for essential OS programs and services (a likely reason why the SP2 upgrade is 300+ MB). It is possible to enable it for other applications but there may be compatibility issues. If a program runs in a marked memory area, Windows closes the program and notifies the user.

Note that a Bugtraq entry reports that the feature is not 'on' by default as noted in Windows documentation. Nicholas Ruff writes, "However, on my computer (Windows XP SP2 32-bit edition + AMD64 Athlon 3000+), hardware supported DEP does *not* work by default, even with "/NoExecute=AlwaysOn".[28] I must add manually the "/PAE" boot parameter inside "BOOT.INI".[29] This information is cause for further investigation and, if it's indeed not enabled by default, is cause for concern. Most home users would not feel comfortable modifying the boot.ini file without help from IT support.

E-mail Handling

Plain Text Mode in Outlook Express.

This option displays messages in rich text format rather than HTML. If this is enabled, malicious code transmitted via email will not be executed in Outlook Express. Outlook Express "processes HTML header scripts in the HTML content…and the MSHTML control automatically executes these scripts."[30] Turning off HTML view prevents malicious code from being executed in this manner. This is not enabled by default, the user must set this option in Outlook Express.[31] Note that enabling this option renders graphics, sounds and other items inaccessible, but protects against possible malicious code execution from carefully crafted images or other files. While this provides a higher level of security, I doubt most users will enable the plain text option without specific instructions and strong recommendations.

The option to limit external HTML content is enabled by default and renders HTML content that has external references blank. Clicking a border area around where image would be, will open a web page to retrieve the content. Microsoft implemented this feature because some businesses were using it to collect valid

email addresses to use for spam. These businesses performed mass mailings of content that contained a blank image that 'phoned home', known as web bugs, and confirmed the receipt of the email, validating the email address.[32] This provides better security for the home user because it stops not only web bugs, but spyware and other malware, and it is already enabled by default.

Attachment Execution Service API Integration.

Microsoft implemented this feature to provide a more "unified approach for attachment security across all Windows applications", rather than use custom applications.[33] It blocks bad attachments, but does more than just checks the file extension.[34] It checks the digital signatures of the publisher and if it is an Untrusted Publisher, will not allow downloading or file execution.

Enhanced Browsing Experience (IE Changes)

Pop-up blocking and the new Manage Add-on window are two of the most obvious changes to IE. Users will also notice changes in prompts when downloading attachments and the addition of a dialog window called the Information Bar. There are more than a dozen items listed in Microsoft's Changes in Functionality white paper that focuses on changes in Internet browsing (Internet Explorer). Some changes were aimed at fixing vulnerabilities and others are aimed at providing better defenses, but many are code changes that are not visible to the user. It's possible, and widely reported, that the modifications will cause sites to break, but note that is not within the scope of this paper to focus on the many possible incompatibilities service pack 2 may cause.

IE File Download Prompt.

Users receive a prompt before any code is downloaded or executed. See the paragraph above on 'Attachment Execution Service API Integration'. This is the sample implementation for IE. Outlook or IE now check the digital signatures of the publisher and if it is an Untrusted Publisher, will not allow downloading or file execution. The user dialog was changed for consistency. And the user always receives a prompt before downloading. Security lies in the users choice or consent and this is not always the best case. On the other hand, downloading software without the user's knowledge is not good security either. At least the user serves as another layer of defense, albeit not necessarily a strong one.

IE Add-on Management and Crash Detection.

This is the new Manage Add-ons window available under the Tools menu. When visiting sites that require an add-on (such as Acrobat Reader or Flash Media Player) a window pops open and asks the user to verify download of the add-on. Manage Add-ons allows users to easily see what add-ons are installed, its publisher, status, and type. It also allows them to easily disable an add-on that may be causing problems. Add-on management is an improvement because Active X controls and browser helper objects are plainly shown in the Manage Add-Ons window. It allows the user to view what is already installed and gives them greater control.

Microsoft reports that many times the cause of IE crashes lies in browser add-ons.[35] The Crash Detection feature is supposed to open a window identifying a particular dynamic link library (dll) file that caused the crash. The user can disable the add-on via the Manager Add-On window. The real power of the feature is for the business enterprise user where a trained administrator can set group policy and enable or disable publishers and add-ons in that manner. Disabling the feature requires either editing the local group policy or changing registry values, not something a typical home user is equipped to handle.

IE Binary Behaviors Security Setting.

An example of a very simple binary behavior is a mouse over behavior. When the mouse is moved over an area on a web page, it may change color or open a menu. Prior to SP2, IE did not place controls over binary behaviors from a restricted zone. SP2 creates a "new URL action setting" in each of IE's zones[36]. All are enabled, except for the restricted zone. If a binary behavior coming from a restricted zone tries to execute, the user will receive an error alert. This provides better security to the home user browsing the internet; however, troubleshooting any problems caused by this change would require experience with group policy or modifying the registry.

IE Information Bar.

This bar or window consolidates and applies consistency across existing dialog boxes such as those encountered when downloading content, Active X controls, and pop-ups. A user can customize display of the information bar and individual features, based on security zone settings. The security aspect of the feature is that it provides another user warning prompt that untrusted software will be downloaded or installed.

Feature Control Registry Settings and Security Zone Settings.

There are several possible security zones that are installed with IE. It's questionable whether the zone organization for providing safe browsing is a good way to approach security for the average user.[37] It puts the burden on the user in deciding whether a site, or its code, is safe or not, and many attacks are able to jump to "trusted" zones and do more damage. The Microsoft white paper on this feature states that it is directed at resolving compatibility issues between an organization's intranet applications and accessing internet sites and applications. It states that this change in SP2 was developed because a "feature control that protects users in the Internet zone may cause an intranet application to stop working."[38].

IE MIME Handling File Type Agreement.

SP2's version of IE addresses potential malicious files that spoof their file extensions. IE checks the Multipurpose Internet Mail Extension (MIME) type against the file extension and if it does not match, shows an error dialog to the user. It does this first by comparing the "MIME type of the cache file to the extension of the cache file"[39]. Then, before the MIME handler executes the file, IE compares "the CLSIDs

of the MIME handler and the extension handler". If these don't match, the user is prompted again whether they really want to download or execute the file. This can prevent many of the spoofing attacks that are so prevalent today.

MIME Sniffing File Type Elevation.

This feature sniffs or reads the bit signatures on certain kinds of files and does not allow the file to be promoted to "a more dangerous file type".[40] This protects users from downloading or executing content from a website that appears to be plain text but is really malicious code.

Pop-up Blocker.

The new pop-up blocker is enabled by default and provides the user with a more controlled browsing environment. If a user wants a pop-up to open, they must click a highlighted bar on top of the IE page. This opens only one pop-up, so the pop-up cannot spawn another. Users can temporarily enable pop-ups, identify sites where pop-ups are always allowed, or block pop-ups entirely. The blocker also places restrictions on the size and placement of allowed pop-ups.[41] Pop-ups may simply SPAM users with unwanted advertisements or they may do more damage by downloading spyware or other types of malware. This is a terrific enhancement to IE that delivers a safer, less intrusive web browsing experience for all users.

Untrusted Publishers Mitigations.

This feature checks for valid signatures when downloading and installing code. It also allows users to block content from specific sites or publishers. This places the burden of determining authenticity on the user because they have the option to allow or disallow the download. On the other hand, a knowledgeable user would benefit from having access to this information that they did not have before.

Windows Restrictions.

This feature addresses issues where websites were spoofed and appeared authentic because the title bar, status, address bar, or some other element was hidden, including the entire window, were not visible. SP2 places more stringent constraints on window positioning. Home users should no longer be deceived by malicious web sites that move or resize windows.

IE Local Machine Lockdown.

Prior to SP2, files on the local file system were automatically part of the Local Machine Security Zone (a less restricted zone than the Internet Zone) and hackers were taking advantage of this vulnerability to remotely execute code in the context of the local user. The Local Machine Lockdown places even more stringent restrictions on HTML code that resides on the users' PC. So if an application runs HTML code from the local file system, some scripts, Java, and Active X controls may not run. The Information Bar will appear with the option to remove the lockdown if desired. This is an enhancement for internet security for home users because it protects against Zone Elevation Attacks. This type of attack was "one of the most exploited vulnerabilities in IE".[42] It removes a large part of responsibility

from the user in an area that the owner should not have to typically worry about.

Zone Elevations Blocks.

Web pages that call more privileged web pages will fail. This is designed to reduce the likelihood that an attacker would gain higher permissions and ultimately the Local Machine Zone. Access to LMZ may give an intruder access to the entire PC and any shares.[43] While Zone Elevations Blocks does provide a layer of defense, users can protect themselves by blocking content from untrusted sites. SANS recommends tightening settings in the Internet Zone and disabling many controls (such as Active X and other types of scripting). Although it is a 2-step process. Set the Security level to High in 'Internet Zone' and this disables all controls except a few that it allows as 'prompt' first before proceeding. However, 'High' security level setting will break many websites. The second step is to add trusted sites to the 'Trusted Sites' Zone. Initially it takes some time and effort in determining which sites are needed and reliable, but I think this is a safer approach to surfing the internet.

Network Protocol Lockdown.

It restricts the type of protocols that IE will handle. Protocols such as local://, file://, shell://, hcp://, ftp:// are generally not used in "rendering HTML with active content"[44]. We can turn these off because they reveal additional ways an attacker may exploit, and the average home user will not likely use these protocols. This Network lockdown feature is not enabled and is designed for Network Administration. The home user will not even know it exists, even though it does have the potential to provide greater security.

Network Protection Technologies

Major changes to network protection technologies are that some services have been disabled, and access control related changes were made in DAVRdr, DCOM and RPC. A discussion of the Windows Firewall may be found under Security Center. The Alerter and Messenger Services, a feature used by network administrators to send messages to desktops has been disabled. This is beneficial to XP Home users because spyware and other malware exploited the Messenger service (unrelated to MSN messenger) form SPAM, or other malware.

WebDAV Redirector (DAVRdr).

DAVRdr is Microsoft's version of an extension to HTTP protocol, and is a feature that allows web server content to be accessed as if it were a file server. It may use Basic Authentication to logon with unencrypted credentials. SP2 changed the default setting for BasicAuth from enabled to disabled. This protects users from their passwords being sent across a network in clear text.[45]

Distributed Component Object Model (DCOM) Security Enhancements.

There were changes in access restrictions and a capability for administrators to disable incoming DCOM activity. This feature is not likely needed on most home PC's and is "the component that the Blaster worm exploited to get at RPC."[46]

Further, Mark Liron of updatexp.com, thinks that DCOM should not be part of the XP OS and his comments coincide with Tom Greene.[47] Liron writes, "DCOM in Windows XP has always been a bad idea! It is a potential source for trouble...most home users are not going to need the DCOM protocol in Windows XP. Some business/corporate users might need it."[48] The enhanced restrictions nevertheless is a benefit to the home user, although it may serve the home user by eliminating it from XP Home Edition.

Remote Procedure Call (RPC) Interface Restriction.

RPC Interface Restriction requires procedure calls to perform authentication and this may protect against worm propagation that relies on anonymous login. A registry key was added that "modifies the behavior of all RPC interfaces… and eliminate remote anonymous access to RPC interfaces on a system…"[49] Authentication in general is an extra layer of protection and makes it more difficult to exploit weaknesses. Microsoft notes that the changes to RPC "is a particularly useful mitigation against worms which rely on exploitable buffer overruns that can be invoked remotely through anonymous connections."[50] This enhancement, coupled with Data Execution Prevention should mitigate buffer overflows. This illustrates how Microsoft has made steps in a defense in depth strategy and it should increase security for the home user.

TCP/IP.

XP SP2 has a restricted ability to send traffic over raw sockets and this reduces the "ability of malicious code to create distributed DoS attacks and limits the ability to send spoofed packets…"[51] Also a limit was placed on the number of "simultaneous incomplete outbound TCP connection attempts."[52] The effects of worms and malicious code often result in many failed or incomplete connection attempts. Network scanners may also do this and may have problems with SP2. When the connection limit is reached, a new event, ID4226 shows up in the Event Log. Home users would not likely check the Event Log in its current implementation and generally Administrators are experts at understanding logging details. However, home users still benefit by this limit on connections because it aids in slowing down the propagation of worms.

Windows Messenger.

Three features were added. Windows Messenger must be added to the Windows Firewall Exception list in order to run. File types other than jpg, txt and gif are blocked. Also, files are blocked if the sender is not in the user's contact list. The home user is then protected from unsolicited and possibly harmful files.[53]

Conclusion

While this was not a comprehensive review of all the many features and fixes of SP2, it did touch the main topics related to security enhancements. The answer to the initial question posed in this paper: "Does SP2 provide in-depth security for the home user?" is both "yes" and "no.". The architectural changes discussed in the feature descriptions above provide another layer of defense against buffer overflow attacks and other malware attacks and their propagation. The changes also reduce spoofing and place controls on downloads. SP2 also introduced some level of authentication where little to none existed. These efforts demonstrate Microsoft's commitment to focusing on security, and also that they addressed security issues at the application, host and network layers. On the other hand, XP places some of the responsibility of mitigating security risks on the user and their responses to the insistent Information Bar. There are some strides in identifying suspicious code such as the MIME file and sniffing capabilities for Outlook, but often, users must decide for themselves if a site should be trusted or not.

There are many more issues that could have been addressed by Service Pack 2, specifically for the XP Home user. SP2 provides IT administrators with security templates in order to deliver a more secure environment to desktops and through Active Directory across domains. I would expect many of the recommendations contained in the SANS Part 5 Guide would be incorporated into SP2. I would hope that at least the eight broadly defined yet essential items noted at the beginning of this paper were addressed, but most were not addressed for the home user. A short analysis of some of SANS recommendations is listed below.

Passwords and Account Lockout

SANS recommends using complex, long passwords that need to be reset in 90 days. There are many potential victim PCs on the Internet, but the hacker is looking for one without a password. It makes their job that much easier. Further, password cracking programs are freely available and are very good at revealing weak passwords. It's good practice to enforce a strong password policy. And, finally, users can deter the password cracker by locking out an account after 5 failed attempts. SP2 home users are not required to create passwords. The strong passwords policy and account lockouts are moot points in XP Home. Adding a feature for password policy and account lockout settings to the Security Center may be a good way to resolve this issue.

Principle of Least Privilege

SP2 used this principle in making architectural changes to DCOM, RPC, and some IE changes. The least amount of privilege, or at least some form of authentication, is given to the user or process in order to operate. However, at an operational level, all XP Home users are still given Administrative privilege, unless a user specifically chooses to set up accounts and groups otherwise. Users should be given administrative privileges on a very limited basis. Apple's Mac OS X uses this principle and at least requires an administrative password to perform any

administrative level function. Microsoft should explore this way of enforcing the principle of least privilege.

Encrypting File System (EFS)

Encryption tools are vital in securing data on a local hard disk and when transferring files. Encrypting important data is another layer of defense, yet EFS is not available for the home user. For example, home users may store bank account information, credit cards, social security numbers and other private information on their hard drives. Encrypting those files ensures that if a hacker where to gain access to them, they would also have to go an extra step and decrypt the data. Tools such as Pretty Good Privacy (PGP) provide secure message exchange and are widely used by businesses and other institutions. There are freely available versions of PGP, but no similar tool is included with Outlook Express. It would be wise for the home user to use PGP for file encryption and confidential email and for Microsoft to include a similar package in XP Home.

Disabling Unnecessary Services

Disabling services reduces the amount of possible vulnerabilities there are to exploit. Windows services are complex and contain dependencies not readily evident to the average user (or administrator for that matter). It's important to test the effects of disabling a service in order to see what dependencies may exist. Greene notes that some readers of The Register disabled needed services and wreaked havoc on their systems[54]. Clearly this is an issue that needs to be addressed. SP2 does disable some services by default (i.e., Messenger and Alerter), but there are likely more that could be turned off or possibly removed for the XP Home user.

Internet Firewall

The Windows Firewall is an improvement over the ICF because it is enabled by default, includes boot-time protection, and provides monitoring with Security Center. I think users are likely served better with a full-featured bidirectional firewall; however, any firewall is better than nothing.

Backups

Recovering from a security breach and learning what went wrong are important issues. Like other Windows versions, XP does have a recovery tool. It also has the ability to roll back to previous versions after installing software or updates. However, XP Home does not include a backup application. Microsoft does, however, provide the option to download a backup utility. Users may be well advised to download it, or at least copy critical information such as bank account registers to a CD-ROM.

Maintenance

Keeping software current is an important part of computer security. The Automatic Update service provides updated software as soon as Microsoft releases it. XP2 does not enable Automatic Update, but does remind users, through the

Security Center, that Automatic Updates should be turned on. I think default installations of XP Home should have Automatic Update turned “ON”.

These features as well as many other SANS recommended settings, such as: disabling the Guest Account (and enforcing a strict password for it), requiring a password-protected screensaver, disabling registry editing tools, disabling auto-play on CD-ROM drive and various browser settings already mentioned, have not been implemented in SP2 for XP Home. Some basic security essentials are simply not addressed for the home user. XP SP2 seems focused on the business enterprise and its staff of administrators. Yes, SP2 provides a more secure environment for the home user and SP2 does provide defense in depth because it addresses security concerns at the application, host and network layers, but it is not comprehensive enough. This was a step in the right direction. However, it would be in the users’s best interest for future security enhancements to give equal focus to the stand-alone user. Ideally, XP Home will become a separate product, dedicated to the home user and protecting their assets with confidentiality, availability, and integrity.

Bibliography

Anderson, Starr and Vincent Abella. "Changes to Functionality in Microsoft Windows XP Service Pack 2." Microsoft TechNet. 09 Aug 2004. 01 Dec 2004 <http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2chngs.mspx>.

Berlind, David. "AMD Asleep at the Wheel?" ZDNet. 15 Aug 2004. 04 Dec 2004 < http://news.zdnet.com/2100-1009_22-5310417.html>.

Blackviper.com Home Page, 2004. Windows XP Home and Professional Service Pack 2 Service Configurations 04 Dec 2004 <http://www.blackviper.com/WinXP/servicecfg.htm>.

Chor, Tony. "IE in Windows XP SP." IE Blog. 10 Aug 2004. 04 Dec 2004 <http://blogs.msdn.com/ie/archive/2004/08/10/212008.aspx>.

"Defense in Depth: A practical strategy for achieving Information Assurance in today's highly networked environments." National Security Agency, Central Security Service. 29 Nov 2004 <http://www.nsa.gov/snac/support/defenseindepth.pdf>.

"A Detailed Description of the Data Execution Prevention (DEP) feature in Windows XP Service Pack 2 and Windows XP Tablet PC Edition 2005." Microsoft Help and Support Center. 03 Dec 2004 <http://support.microsoft.com/kb/875352#4>.

Foley, Mary Jo. "PC Makers Seize the Reins of XP SP2 Security". eWeek. 20 Oct 2004. 03 Dec 2004 <http://www.eweek.com/article2/0,1759,1681028,00.asp>.

Galloway, Jon. WeBlog. "XP SP2, IE, the Local Machine Zone Lockdown, and you". 07 Dec 2004 <http://weblogs.asp.net/jgalloway/archive/2004/08/20/218123.aspx>.

Greene, Thomas C. "SP2 on XP Home." The Register. 17 Sep 2004. 05 Dec 2004 <http://www.theregister.co.uk/2004/09/17/xphome_sp2/>.

Greene, Thomas C. "WinXP SP2 = security placebo?" The Register. 09 Sep 2004. 23 Nov 2004 <http://www.theregister.co.uk/2004/09/02/winxpsp2_security_review/>.

Greene, Thomas C. "Reg Readers Sabotage their Windows Boxes." The Register. 14 Sep 2004. 23 Nov 2004 < http://www.theregister.co.uk/2004/09/14/reg_readers_windows/>.

Lee, Wei-Meng. "An Inside Look at XP SP2." Unwired. 04 May 2004. 02 Dec 2004 <http://www.windowsdevcenter.com/pub/a/windows/2004/05/04/SP2RC1.html>.

Liron, Mark. "DCOM Windows XP: Do You Need It?" www.Updatexp.com. Sep 2003. 04 Dec 2004 <http://www.updatexp.com/dcom-windows-xp.html>.

Microsoft Security at Home, Home Page 2004. Microsoft Corporation. 04 Dec 2004 <http://www.microsoft.com/athome/security/default.mspx>.

Microsoft Windows XP, Using Windows XP, Security and Privacy Home Page. "Understanding Windows Firewall." 04 Aug 2004. 07 Dec 2004. < http://www.microsoft.com/windowsxp/using/security/internet/sp2_wfexceptions.mspx>.

Minasi, Mark. "Windows XP Service Pack Presentation." 02 Nov 2004. 03 Dec 2004<http://www.minasi.com/sp2info/xpsp2color.pdf>.

.

Rash, Wayne. "Windows XP SP2: A Bandage Not a Panacea." InfoWorld. 12 Nov 2004. 04 Dec 2004 <http://www.infoworld.com/article/04/11/12/46TCsp2_1.html>.

Ruff, Nicholas. "Hardware Support for XP DEP Not enabled by Default?" Security Focus, 11 Nov 2004, 07 Dec 2004 <http://www.securityfocus.com/archive/1/382002>.

SANS Institute. Track 1 – SANS Security Essentials Defense-In-Depth Version 2.2. Volume 1.2. SANS Press, Jan, 2004.

SANS Institute. Track 1 – SANS Security Essentials Windows Security Versions 2.2. Volume 1.5. SANS Press, Jan, 2004.

"Security Improvements in Windows XP Service Pack 2." US-CERT National Cyber Alert System, Cyber Security Alert SA04-243A. 30 Aug 2004. 29 Nov 2004 <http://www.us-cert.gov/cas/alerts/SA04-243A.html>.

Semilof, Margie. "XP refresh gives rise to plethora of Group Policy settings." SearchWin200.com. 01 Sep 2004. 29 Nov 2004<http://searchwindowssecurity.techtarget.com/originalContent/0,289142,sid45_gci1006416,00.html>.

Spanbauer, Scott. "Tweak Windows XP SP2 Security to Your Advantage: Fine-tune the settings in Microsoft's recently released Windows XP Service Pack 2." PC World Magazine, Oct 2004. 04 Dec 2004 <http://yahoo.pcworld.com/yahoo/article/0,aid,117422,00.asp>.

"Support Webcast: Understanding Microsoft Windows XP Service Pack 2." Microsoft Help and Support. 24 Sep 2004. 05 Dec 2004 <http://support.microsoft.com/default.aspx?scid=kb;en-us;883733>.

"Windows XP". From Wikipedia, the free encyclopedia, 2004. 06 Dec 2004 <http://en.wikipedia.org/wiki/Windows_XP>.

Windows XP Home Edition Must be Made More Secure Home Page. Steve Gibson. 03 Oct 2003. 06 Dec 2004. <http://grc.com/dos/sockettome.htm>.

"Windows XP Service Pack 2 Technologies Review". Microsoft Windows XP, Using XP. 04 Aug 2004. 05 Dec 2004 <http://www.microsoft.com/windowsxp/sp2/technologiesoverview.mspx>.

Endnotes

[1] Anderson, Starr and Vincent Abella, "Changes to Functionality in Microsoft Windows XP Service Pack 2", Microsoft TechNet, 09 Aug 2004, 01 Dec 2004 <http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2chngs.mspx >, Part 1, page 3.

[2] Microsoft Tech Net Page, "Windows XP Security Guide", 15 Aug 2004, 09 Dec 2004 < http://www.microsoft.com/technet/security/prodtech/winclnt/secwinxp/xpsgch01.mspx>.

[3] Microsoft Security at Home, Home Page 2004, Microsoft Corporation, 04 Dec 2004 <http://www.microsoft.com/athome/security/default.mspx>.

[4] Greene, Thomas C, "WinXP SP2 = security placebo?" The Register, 09 Sep 2004, 23 Nov 2004 <http://www.theregister.co.uk/2004/09/02/winxpsp2_security_review/> p 7.

[5] SANS Institute, Track 1 – SANS Security Essentials Windows Security Versions 2.2, Volume 1.5, (SANS Press, Jan, 2004) 11-182.

[6] SANS Institute, Track 1 – SANS Security Essentials Defense-In-Depth Version 2.2, Volume 1.2, (SANS Press, Jan, 2004), p. 12.

[7] Greene, Thomas C, "WinXP SP2 = security placebo?" p 4.

[8] Greene, Thomas C, "Reg Readers Sabotage their Windows Boxes", The Register, 14 Sep 2004, 23 Nov 2004 < http://www.theregister.co.uk/2004/09/14/reg_readers_windows/>.

[9] Blackviper.com Home Page 2004, Windows XP Home and Professional Service Pack 2 Service Configurations, 04 Dec 2004 <http://www.blackviper.com/WinXP/servicecfg.htm>.

[10] Greene, Thomas C, "Win XP SP2 = security placebo?" p 2.

[11] Greene, Thomas C, "Win XP SP2 = security placebo?" p 2.

[12] Spanbauer, Scott, "Tweak Windows XP SP2 Security to Your Advantage: Fine-tune the settings in Microsoft's recently released Windows XP Service Pack 2," PC World Magazine, (Oct 2004. 04 Dec 2004) <http://yahoo.pcworld.com/yahoo/article/0,aid,117422,00.asp>.

[13] Minasi, Mark, "Windows XP Service Pack Presentation," 02 Nov 2004. 03 Dec 2004<http://www.minasi.com/sp2info/xpsp2color.pdf>.

---

[14] Greene, Thomas C, "Win XP SP2 = security placebo?" p 7.

[15] Microsoft Windows XP, Using Windows XP, Security and Privacy Home Page. "Understanding Windows Firewall." 04 Aug 2004. 07 Dec 2004. <http://www.microsoft.com/windowsxp/using/security/internet/sp2_wfexceptions.mspx>.

[16] Greene, Thomas C "SP2 on XP Home".

[17] Foley, Mary Jo, p 1.

[18] Microsoft Windows XP, Using Windows XP, Security and Privacy Home Page. "Understanding Windows Firewall." 04 Aug 2004. 07 Dec 2004. <http://www.microsoft.com/windowsxp/using/security/internet/sp2_wfexceptions.mspx>.

[19] Greene, Thomas C, "Win XP SP2 = security placebo?" p 7.

[20] Foley, Mary Jo, "PC Makers Seize the Reins of XP SP2 Security", eWeek, 20 Oct 2004, 03 Dec 2004 <http://www.eweek.com/article2/0,1759,1681028,00.asp>.

[21] Minasi, Mark, "Windows XP Service Pack 2 Presentation", p 3.

[22] Spanbauer, Scott.

[23] Anderson, Starr and Vincent Abella, Part 3, p 5.

[24] Minasi, Mark, "Tech Page Issue #41".

[25] Microsoft Help and Support Center., Knowledge Base Article 875352#4

[26] Berlind, David.

[27] Microsoft Help and Support Center., Knowledge Base Article 875352#4

[28] Ruff, Nicholas.

[29] Ruff, Nicholas.

[30] Anderson, Starr and Vincent Abella, Part 4 p 3.

[31] Anderson, Starr and Vincent Abella, Part 4 p 3.

[32] Anderson, Starr and Vincent Abella, Part 4 p 4.

[33] Anderson, Starr and Vincent Abella, Part 4 p 4.

[34] Minasi, Mark, “Windows XP Service Pack 2 Presentation”

[35] Anderson, Starr and Vincent Abella, Part 5, p 10

[36] Anderson, Starr and Vincent Abella, Part 5, p 15

[37] Greene, Thomas C, “SP2 on XP Home”.

[38] Anderson, Starr and Vincent Abella, Part 5, p 28.

[39] Anderson, Starr and Vincent Abella,Part 5, p 48.

[40] Anderson, Starr and Vincent Abella, Part 5, p 51.

[41] Anderson, Starr and Vincent Abella, Part 5, p 60-63.

[42] Galloway, Jon.

[43] Anderson, Starr and Vincent Abella, Part 5, p 65.

[44] Anderson, Starr and Vincent Abella, Part 5, p 70.

[45] Anderson, Starr and Vincent Abella, Part 3, p 11-13.

[46] Greene, Thomas C, “Win XP SP2 = security placebo?” p 1

[47] Liron, Mark.

[48] Liron, Mark.

[49] Anderson, Starr and Vincent Abella, Part 2, p 9.

[50] Anderson, Starr and Vincent Abella, Part 2, p 9.

[51]Anderson, Starr and Vincent Abella, Part 2, p 8

[52] Anderson, Starr and Vincent Abella, Part 2, p 8

[53] Anderson, Starr and Vincent Abella, Part 2, p 24

[54] Greene, Thomas C, “Reg Readers Wreak Havoc”.

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event