Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

XP - The Future of Secure Operating Systems?

Finally, the future has arrived! With the launch of Microsoft's anxiously awaited Windows XP, we can all breath a little easier as Security Administrators. Alright, so we all know that is an utter lie but maybe, just maybe our jobs will be a little bit easier because of XP. Rumor has it that this is the most stable and secure version of Windows that Microsoft has ever released. For most of you, that isn't really saying much. The point is though that the product is improving are getting better. Of course there are vulne...

Copyright SANS Institute
Author Retains Full Rights

AD
nitrosecurity Log Management

Practical Assignment 1.2f

XP – THE FUTURE OF SECURE OPERATING SYSTEM'S?

Justin Coburn

November 20, 2001

Finally, the future has arrived! With the launch of Microsoft's anxiously awaited Windows XP, we can all breath a little easier as Security Administrators. Alright, so we all know that is an utter lie but maybe, just maybe our jobs will be a little bit easier because of XP. Rumor has it that this is the most stable and secure version of Windows that Microsoft has ever released. For most of you, that isn't really saying much.

The point is though that the product is improving are getting better. Of course there are vulnerabilities in XP, there were vulnerabilities in Windows 95, Windows 98, Windows NT, etc., etc., etc. But if you take a step backwards and compare how much work you have to do to secure a Windows 9x machine, if it is possible, and how much work you have to do to secure a Windows 2000 machine I believe its pretty obvious the point I'm trying to make here.

The world will always be full of Microsoft critics; I have come to realize that is almost a universal law. In fact, in numerous ways I am also one of them. But it's time to step up to the plate and admit that things are moving in a positive direction. XP is a major step in that direction and the following explains why.

FILE SYSTEM

Let's begin simply. Everyone knows by now that NTFS is much more secure than FAT32. Of course this is obvious to everyone out there but it is a beginning. XP implements the same file structure as Windows 2000. The ability to set permissions on files and folders is a major security tool. XP expands on this ability and the ability of 2000 to use encryption on these files and folders.

The Encryption File System (EFS) was a major enhancement in Windows 2000. The ability to encrypt files and even whole folders allowed a single user to keep other users from reading their files. Though EFS is based on public-key encryption, Windows XP makes this feature a little easier to use. If the user does not already have one, EFS will automatically generate a certificate and an encryption key pair for the user. Another advantage of XP and EFS is that it can use either the DESX or 3DES encryption algorithms.

This process is completely transparent to the user. If they need to use one of the files, Windows will decrypt the file and open it for use. Once the file is closed again, it encrypts it back for protection. But XP also improved on one other area of the EFS from Windows 2000, encrypting Offline Files and Folders. So say you were a traveling user who needed to access sensitive data from the road. You frequently download and synchronize your documents for easy viewing but before, those client-side cached

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

documents could not be encrypted. Therefore if your laptop was stolen, the attacker would have full access to the offline files database. But with XP, you can encrypt or decrypt the whole database. Therefore, only if the attacker gains access to your key can he/she decrypt your sensitive offline database cache.

INTERNET CONNECTION FIREWALL

One of the major new features of Windows XP is the Internet Connection Firewall (ICF). Though the product is limited in its capabilities, discussed further below, it does add a nifty enhancement to security for business users. Defense in Depth is an approach everyone is trying to implement to its fullest possible extent. ICF provides host based firewall protection on all of your network machines, for free.

So what exactly does ICF do? In affect, it attempts to make your computer invisible to the outside world, the Internet. It monitors incoming packets to try and determine whether or not they are malicious or a valid request. Notice that I did not say anything about outgoing packets. ICF does absolutely nothing to protect the rest of the Internet from your machine. Therefore if your machine is infected with a trojan horse, you will become just another zombie in a war against good.

But ICF is still useful. It has the capabilities to protect dial-up connections or cable/DSL internet access for the home users out there and LAN or VPN protection for the business users. By default, you can block FTP, ICMP, HTTP, ICMP and a number of other protocols from accessing your machine. You also have the option to block other services if you so choose. ICF also has configuration for logging dropped packets or successful attempts. Auditing is quite simple since the file is stored in basic log format, but the downfall is that it doesn't always provide all the information that other personal firewall logs do.

The only question that remains in my mind is why Microsoft didn't take the extra incentive to build an anti-virus utility into the firewall or operating system as well? Most likely a corporate, profit incentive move but don't be surprised to see this option in a future version of Windows.

SECURITY POLICIES

Introduced in Windows 2000, local and group policies make managing security on machines a much simpler task. Doing away with stressful registry hacks, the graphical user interface provides ease of use and a much better understanding of what it is that you are actually doing.

Windows XP implements the same basic setup as Windows 2000 did, but with a few new twists in the Security Options menu. The menu is now organized by grouping the policies into what type of service they affect. With groupings such as Network Security and Devices it is much easier to sort through what needs to be set and what doesn't on your box.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Of course this also means that this can all be integrated with Active Directory. The plan according to Microsoft is for Windows .NET server to be released in the future. This is the OS to take over for Windows 2000 Server and Advanced Server. But for the time being, XP works very well on a Windows 2000 domain. By using group policy to roll out a standard set of security policies for all of the machines on your network, you should be able to sit back with your feet propped on the desk.

In affect, with 2000 and XP Group Policy, you are running an SMS server. Group policy allows you to not only configure the security policies, but also to roll out service pack upgrades, scripts, and even run software installs across the network. Of course the software installs must be .msi files, but a small price to pay at this point for an excellent feature. There are also modules to configure IPSec policies and data recovery agents for the EFS mentioned above.

AUTOMATIC UPDATES

Depending on your point of view, this can be a good feature or a very bad one. Allowing a machine to automatically download and install updates from Microsoft can be a dangerous endeavor. Most administrators prefer to thoroughly test these updates before they roll them out on there live stations. But what about the administrators who are unable to implement Active Directory or SMS in order to push the updates out to their users, are the user's actually going to install the updates? Automatic updates provide a means of being sure that these updates are being installed on your workstations.

This option is configurable from standalone stations to full integrated domain workstations. On standalone machines, the service can be setup to not download any updates at all, or you can configure it to only download the latest updates. The user may then install them at a convenient time. The final option allows for any updates found to be downloaded and installed automatically.

REMOTE ASSISTANCE

A completely new feature for Windows XP is the ability to share your desktop and applications via Windows Messenger or Outlook Express 6. In the past, this feature was only available via third-party applications. The ability to do this securely is absolutely beyond the scope of this paper and should be researched thoroughly. Some issues that come to mind are whether you can change the default port numbers that the programs use and many other questions need to be answered.

I was able to determine that this feature can be disabled for computers on a domain by using Group Policy. This is an excellent option for administrators who do not wish to utilize this feature. Yet this feature is a great time saver for larger corporations who have many users in various locations. Hopefully Microsoft had the foresight to include configuration options for high security standards.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

PASSPORT AND .NET

Privacy advocates are having a field day with this new feature/burden. Probably the most annoying feature and ideally not the most secure is the "required" implementation of Microsoft's .NET Passport service with XP. When XP is launched initially, any user who attempts to use Windows Messenger will be prompted to sign up for a Windows .NET passport. They will be periodically prompted from there on to sign up as well. According to some sources, the prompt eventually desists, but there is no guarantee on the time length.

Marc Rotenberg, the executive director for EPIC, will be asking the FTC to open an investigation into the various ways in which Microsoft attempts to gain personal information from its users. Central to this issue is .NET and passport which are both heavily implemented into XP and will definitely be implemented into Windows .NET Server which will be the next release.

Most corporate users should not be using the majority of these products while on corporate time. Passport is intended to store information of a personal nature, not a corporate one. Microsoft should have left this feature out, or at least provided an easy way to disable it in the Professional addition of XP.

BIOMETRIC, WIRELESS, AND SMARTCARD SUPPORT

Windows XP definitely includes enhancements for new technological advances in the field. With better support for smart cards and biometrics, Windows XP allows for more secure authentication methods if available. XP is also shipping with the ability to support the new wireless authentication standard, 802.1x. This comes on after the discovery of vulnerabilities that have been found in the previous standard, 802.11b.

XP supports the use of smart cards in various degrees. It has added the ability to require smart cards to run certain administrative programs. This can be applied to critical files such as CMD.exe or CSCRIPT.exe and WSCRIPT.exe. This could potentially prohibit a hacker who gains access to a box remotely from running the programs without finding a way around the smart card authentication.

XP also supports the use of smart cards while using terminal services. Many administrators currently use terminal services in order to access a remote server or any server that isn't in close physical vicinity. Now an administrator can require that terminal service authentication be done over smart cards. Prior to XP, Kerberos would need to be used in order for a 'secure' authentication channel.

Support for Biometric devices comes through another new feature in Windows XP, fast user switching. This allows for users to log on simultaneously, without having to lose information they were working on. This can be integrated with Biometric devices such as fingerprint or iris scans.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

RAW SOCKETS

Yet, all is not well with everyone and Windows XP. Steve Gibson, of Gibson Research Company has been in a battle with Microsoft ever since Whistler Beta (Microsoft's beta name for Windows XP). Mr. Gibson believes that because of the default configuration of XP to have all users be established as Administrators that Distributed Denial of Service (DDoS) attacks will become and everyday adventure once XP has established itself in homes across the country.

As stated, all users become Administrators by default on Windows XP. And because of the design of XP, this means that all users have direct access to raw sockets, an obviously dangerous dimension. If the machine is ever compromised, the distributed denial of service attacks could take down entire networks very easily and the administrators would never be able to determine where the attacks are coming from. If the attacker has access to the raw sockets, they also have the ability to spoof the IP addresses that they are attacking from.

Microsoft maintains their position on raw sockets. The underlying reason for granting all users Administrator access is to support legacy applications that were designed to run on Windows 9x and Windows ME systems. Those operating systems did not have user authentication built in and therefore neither did any of their applications. If Microsoft had designed XP to create user groups instead of administrator groups then the majority of the programs for 9x and ME would not run for the normal XP user. Microsoft also claims the goal is to keep malicious code from every reaching the machine, thus the implementation of ICF.

But this hasn't deterred Mr. Gibson. He maintains that it is perfectly acceptable for the system to have full access to raw sockets, but under no circumstances should any user, administrator included have that kind of access. And I would have to agree with him on the fact that it is just foolish to think that just because your goal is to keep malicious code from ever reaching the box, you shouldn't have a backup protection system in place.

CONCLUSION

Windows XP is definitely not the end-all for secure operating systems. There are problems, holes, vulnerabilities like there are in all other operating systems. Microsoft has gone a long way to include easier implementation and enhanced security features in this version of Windows though. Most of the issues revolve around Privacy and some highly technical points (.NET and raw sockets) but aside from those, the security is improved over that of Windows 2000 and much improved over the security of Windows 9x and NT.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

REFERENCES

"Privacy advocates take aim at Windows XP", Olsen, Stefanie and Junnarkar, Sandeep, CNET News.com, http://news.cnet.com/news/0-1005-200-6676181.html

"Windows XP Home Edition Must be Made More Secure", Gibson, Steve, Gibson Research Company, http://grc.com/dos/sockettome.htm

"Battle rages over Windows XP Security", Wearden, Graeme, ZDNet (UK), http://www.zdnet.com/zdnn/stories/news/0,4586,2770517,00.html

"Introduction to the Microsoft Windows XP Firewall", Snitchler, Matt, SANS Institute Information Security Reading Room, http://www.sans.org/infosecFAQ/win/XP_firewall.htm

"Windows XP Professional: Secure", http://www.softcat.co.uk/Templates%20for%20Softcat%20Content/Win_XP/xp_secure.htm

"Windows 2000 EFS", Ahmad, Zubair, Windows 2000 Magazine, http://www.win2000mag.com/Articles/Print.cfm?ArticleID=7977

"What's New in Security for Windows XP Professional and Windows XP Home Edition", Microsoft Corporation, http://www.microsoft.com/windowsxp/pro/techinfo/planning/security/whatsnew/WindowsXPSecurity.doc

"Windows XP to offer wireless security", Wong, Wylie, CNET News.com, http://news.cnet.com/news/0-1004-200-5255030.html?tag=owv

"Windows XP may spur biometrics", Verton, Dan, CNN.com, http://www.cnn.com/2001/TECH/ptech/10/30/windowsxp.biotmetrics.idg/index.html

"Former federal agent calls XP a threat to national security", Fontana, John, Network World, http://www.nwfusion.com/cgi-bin/mailto/x.cgi

"Windows XP: A Firewall for All", Salkever, Alex, Business Week Online, http://www.businessweek.com/bwdaily/dnflash/jun2001/nf20010612_227.htm

"How will Windows XP cope with security?", Andress, Mandy, InfoWorld, http://www.itworld.com/Comp/2218/IWD010514tcwindowsxp/

"Government should block XP release", Gillmor, Dan, Mercury News, http://www.siliconvalley.com/docs/opinion/dgillmor/dg080301.htm

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

"Windows XP Inside & Out", Spanbauer, Scott, PCWorld.com,
http://www.pcworld.com/resource/printable/article/0,aid,63223,00.asp

© SANS Institute 2001, Author retains full rights

Last Updated: May 22nd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**