Global Information Assurance Certification Paper

Beginning to End – Personal Computer and Workstation Security

By Paul Reeder

SANS Security Essentials
Version 1.2f
Original Submission
East Coast SANS Conference, Washington, D.C.

Introduction

Extremely high-powered computers and fast Internet access used to reside solely in the purview of large businesses and public organizations. However, typical consumers have experienced and taken advantage of steep drops in the price of technology during the mid- to late- 1990's to outfit themselves with personal computers that rival the power of the enterprise file servers of yesteryear. Because of their increased power, application resources, and broadband access, the typical personal computer is relied upon to perform a greater number of functions, as well as store a greater amount of information. These factors have combined to make the typical personal computer a frequent target of erstwhile Internet-abusive attackers. There are numerous reasons a personal computer is a valuable, and somewhat opportunistic, catch for an attacker: their processing power and broad band access make them a useful tool for carrying out attacks against other computers, they often hold detailed personal or sensitive information that is relatively easy to access, and most are running the same operating system with the same vulnerabilities.

There is a great deal of discussion and focus regarding the protection of large enterprise-wide information resource systems. However, because personal computers do not have the same degree of apparent intrinsic value, they are rarely protected with the same tenacity as enterprise-wide systems. Unfortunately, threats to personal computers are numerous and varied. They include: trojan horses that are installed by attackers or unwitting users, internet and email worms, macro viruses, buffer overflow attacks, and an overall transparency that allows attackers to see what applications are installed and what information is stored on the hard drive. This list is by no means comprehensive as new vulnerabilities are discovered regularly, and old vulnerabilities continue to be exploited with startling frequency. Considering the potential for personal computer vulnerabilities to allow attacker traversals to general support networks or major applications, these exploits are particularly disconcerting.

However, there are a number of protective measures that can be employed to mitigate the vast majority of published vulnerabilities. A key element of a majority of these measures is that they are free. There are three collections of protective measures this paper will discuss. The first collection of protections centers around the configuration and preference settings that are available on most personal computers. The second collection shifts the focus to tailor made personal computer security applications and tools. The third collection revolves around specific user behaviors that can make or break personal computer security. Individual security measures do provide a certain measure of protection. However, to be truly effective, a multi-modal personal computer security plan should be employed using different measures to provide a defense in depth.

Application and Operating System Issues

To a certain extent application developers either saw the potential damage that could be caused to their systems by malicious codes and activities, or they had enough

bad experiences with them to warrant a degree of caution. The end result is a certain amount of security built into applications and operating systems either by design, or by the careful choice of configuration settings. This section will focus on the Microsoft™ collection of applications and operating systems. This is not intended in any way to slight manufacturers, but rather recognizes the apparent majority of personal computers that utilize Microsoft™ products, and a desire to not write a book. However, the similar features employed by different application manufacturers create a similarity in the utilization of their built-in security and configuration settings.

The first setting to consider is the protection from malicious macros that can run privileged commands on a personal computer. On most Windows™ applications, the Options choice under the tools menu includes a selection for Macro Virus Protection. This is either found under the Security Tab or the General Tab, depending on the version. Newer versions of Windows™ go a step further allowing macro authors to digitally sign their macros so that a trust relationship can be built between users. This does not indicate an inherent trust in a macro, rather, the trust is in the user that digitally signed it. When considering application security, also remember that most Windows™ applications allow you to password protect any files that you save. This is accomplished by setting a password to modify or open a file under the Options button of the Save As menu.

The Windows™ operating system does not actually delete a file when the delete key on the keyboard is pressed. Instead, it changes the way that file is referenced on the File Allocation Table (FAT) or NT File System (NTFS), noting that the hard drive space the file occupied is available again for use. This allows the undelete functions built into Windows™ to operate, but may also allow an attacker to gain information the user thought had been deleted. For potentially sensitive information, such as financial information, applications specifically designed to securely delete the information should be used. Similarly, many applications generate temporary files that are used to recover working files in the event of a system or application crash. These files contain information that is very similar to the information in the working files, and should be sought out and deleted specifically as well. Temporary files can often be quickly identified using Windows Explorer™ to search for file names ending with .tmp, or file names that begin with the tilde (~) character.

Because Windows™ was designed to integrate easily into a networked environment, individual personal computers that are Windows™ based can be configured to share files and resources. Unless there is a specific need for this feature (i.e. the computer resides on a Local Area Network (LAN) and the LAN users depend on this computer for some functionality), this feature should be disabled. Enabling this feature will more easily allow attackers to view files and resources on the target computer. While on the subject of the Windows™ based personal computers, it is critical to maintain patch currency. New patches for these systems are released on a fairly regular basis, and it is generally inadvisable to wait more than a month without checking for new patches. This includes patches for specific applications, as well as the underlying operating system. Though the NT™/2000™/XP™ platforms are often more directly affected by new patches, even the 95™/98™/Me™ systems require the occasional patch. The importance of maintaining patch currency was illustrated recently by the Code Red and Nimda worms. These worms took advantage of vulnerabilities

that patches had been released to repair several weeks prior to the onset of these worms. Manufacturer patches should be checked for at least monthly, and, when possible, tested prior to being installed. If they can not be tested, a recovery program should be created for the computer, in case the patch has unexpected consequences.

The application of greatest concern is the Web browser. This application is the face that most users are presenting to the Internet, so to speak. Therefore, it should be configured securely and kept current in terms of patches and versions. The first item to check on Internet Explorer[tm] (again the focus is on Microsoft[tm] products) is the encryption cipher strength. This can be found by selecting the About option on the Help menu. The cipher strength should be at least 128 bit. If it is not, the easiest way to upgrade this is to upgrade the Internet Explorer[tm] version. Versions 5.5 and above default to 128 bit, and version upgrades are free downloads from the Microsoft[tm] Web site. Stronger cipher strengths are particularly important for shopping online, especially as this the volume of online sales is rising rapidly. Internet Explorer[tm] also has configurable security and privacy settings. They can both be accessed using the Internet Options option on the Tools menu. Security and Privacy each have their own tabs. Both Security and Privacy have preset security policies they can be associated with: low, medium, or high (although Privacy adds “Allow All Cookies”, “Block All Cookies”, and “Medium High”; Security adds “Medium Low”), or the user has the option of customizing their Security and Privacy policies using a series of toggle switches for different options. The Security section primarily controls the rights a Web server has to execute code (Java or ActiveX), download files, or install applications on a personal computer. Generally a security setting of Medium is a good idea here. A Medium security setting will prevent Web servers from being able to execute commands on the client computer without first prompting the user. In addition, it prevents any unsigned ActiveX controls from executing. A setting of High will arbitrarily block downloads and command executions without prompting the user, which can severely diminish Web site functionality. This should only be used if the computer may be used in environments where malicious attacks are imminent or in progress. Conversely, a setting of Low will allow all code to be executed, downloaded, or installed on a computer without prompting. Though this setting could be used relatively safely for Web sites that are absolutely trusted with the addition of encrypted communications, it is putting all security trust with another computer, and should thus be avoided.

For computers used entirely for personal use, the user manages the privacy settings. However, for organizationally owned computers, or other computers that are used for purposes other than personal, the privacy settings are often mandated by the organization. In fact, there are minimum standards of privacy and protection that are mandated legislatively or by Federal policy for some types of information. These standards cannot be extended for computers intended solely for personal use. The Privacy settings generally revolve around Web sites’ use of cookies. Some cookies are session cookies and only last for as long as the connection is maintained between the personal computer and the Web server. Others are persistent and stay on your hard drive until manually deleted. All cookies may contain private information (such as information entered into a Web form). These cookies should contain a privacy policy that prevents them from being shared with other Web sites. Internet Explorer[tm] can automatically check for this policy, and this feature is enabled in almost all Privacy

settings, except for the “Accept All Cookies” option. The difference lies in how the cookies are handled. The High option will block all cookies without a privacy policy, while all other settings (except “Accept All Cookies” and “Block All Cookies”) will only block third party cookies without privacy policies. In addition, the settings manage how your computer will handle cookies that contain personally identifiable information. High and Medium High will block cookies using personally identifiable information without your consent. The Low setting will restrict third party cookies with personally identifiable information, and does not address first party cookies. The Medium setting blocks third party cookies with personally identifiable information without user consent, and only restricts first party cookies. Using the higher security settings when surfing the Web can be disruptive, though not so disruptive that it would be a good idea to not restrict cookies, allowing them to be read by other Web sites. Most reputable Web sites will function even if the browser is using high privacy settings, so this is the setting recommended. Another note about privacy and Internet Explorer[tm] is the AutoComplete[tm] option that can be found under the Content tab of Internet Options. It is important to remember that password, Web form, user ID, or Web address that can be automatically completed is stored on your hard drive. If an attacker compromises a hard drive, they would have access to all of this information. Though the information is not necessarily sensitive, at the very least it provides information about Web surfing habits and activities. Though this is not inherently bad, for some people it is analogous to having someone watching them through the window of their house. The AutoComplete option is very easy to disable, and doing so will raise the degree of privacy a user can have on the Web.

Cookies and other temporary Internet files can be easily removed in Internet Explorer[tm] versions 5.5 and above. The Internet Options choice under the Tools menu contains a General tab. The General tab has buttons for Deleting Cookies and Deleting Files, as well as for Clearing History of visited sites. Periodically clearing these files out will free up hard drive space (sometimes temporary Internet files are large graphics images) and make it more difficult for Web surfing habits to be tracked.

Another application of concern because of its use for data interchange is the mail application. Viruses and worms are commonly transmitted via email, and sometimes do not have to be executed to in order to spread. There are a number of preventive measures that can be applied to prevent malicious code from spreading using the mail engine, though many of them are external to the mail program and are discussed elsewhere in this paper. However, directly related to Outlook[tm] is the use of the preview pane. The preview pane allows users to view the contents of a mail message without actually opening the message. Unfortunately, some worms can execute themselves if they are only visible in the preview pane (even without being detached from the message or executed by the user). Deselecting the Preview Pane toggle switch under the View menu will disable the preview pane and can help prevent email worms from spreading.

Though not an application specific issue, passwords are often the first line of defense between access to a personal computer and an attacker. There are a number of applications available, often for free, that can quickly guess a weak password. A weak password is any word that is found in the dictionary, any word found in the dictionary with a common letter to number swap (i.e. replacing “l” with a “1”), any word

or phrase that can be easily associated with the user, or any password of less than eight characters. A password should be as strong as its position as the first line of defense would indicate. Strong passwords contain characters from throughout the keyboard, such as special characters like: !@#$%^&*()_+:{~. The use of these characters in a password greater than eight characters does not guarantee that a password cannot be guessed by a password cracking program, but it does guarantee that guessing the password will take significantly longer. Combined with frequent password changes (at least every 90 days for a general user and every 30 days for administrators), it is likely that an account's password will be changed before it is guessed. Password policies in organizational environments can be enforced automatically with a variety of possible configuration settings in Windows[tm] –based servers. Configuration settings can be made to prevent password reuse, set change frequency, and other options. This policy will often extend to NT[tm] based computers in the same environments as most users will keep their network and local passwords synchronized. However, Windows[tm] operating systems, especially those that are NT[tm] based, create a number of default accounts. The default Guest account does not have a password, and should be disabled. The default Administrator account cannot be disabled, but also has a blank password by default. Though the password must be created during the installation, a popular choice tends to be "Administrator". This is not a good idea, as it is often the first guess that many attackers make. The Administrator password should be well constructed and changed often.

Security Specific Applications

There are many classes of applications that are designed specifically for security at the personal computer level. The old mainstay security application is the traditional anti-virus software. Two of the more popular anti-virus manufacturers are Symantec[tm] and McAfee[tm]. New viruses and worms are identified daily, and new anti-virus software will protect against both. In addition, new anti-virus applications will scan for malicious payload coming into the computer, as well as in files or data that are leaving the computer. This helps prevent the spread of both viruses and worms. The frequency at which new viruses and worms are identified dictates that anti-virus signatures be updated at least weekly. This is usually accomplished by downloading the new signatures from the manufacturer's site, and usually paid for on a subscription basis. Both the McAfee[tm] and Symantec[tm] Web sites provide online security scanning for personal computers that are connected to the Internet. These scans will often detect the presence of viruses and worms, in addition to providing the user with an idea of what vulnerabilities may be present on their computer.

Personal firewalls may be growing the fastest in terms of popularity for personal computer security and are absolutely critical for the "always on" Internet connections such as Digital Subscriber Lines (DSL), Cable Modem access, and Satellite connections. There are reports that broad band service providers are not always willing or able to work with customers using personal firewalls. However, that alone should not prevent a user from employing a personal firewall, especially if their computer is going to be connected to the Internet for long periods of time. Broad band service providers

are becoming more cooperative with the use of a personal firewall, in some cases forming partnerships with personal firewall manufacturers, or simply by encouraging their customers to use one. When the service providers are not willing to provide support for the use of a personal firewall, that does not mean the firewall cannot be used. Personal firewalls are extremely configurable, and will likely work with almost any broadband connection, but may require experimentation and tweaking to find the right combination of access and security. If the broadband connection will not function with the firewall, and the service provider can provide no assistance, it is important to remember that most areas are serviced by more than one provider, and a service change should be considered.

Popular personal firewalls include ZoneAlarm[tm], BlackICE [tm], Sygate [tm], Tiny Firewall [tm], and others. Many personal firewalls have free versions that can be downloaded and installed from their manufacturer Web sites, though their commercial (not free) versions provide more functionality. At a minimum, these firewalls should provide logging for failed inbound and outbound connections, and the ability to outright block selected Internet traffic either originating from the host computer, or from the Internet. This feature can be critical to the identification of Trojan Horses and Viruses active on the host computer, as well as preventing attackers or worms from discovering any information about the host computer. The new version of Windows [tm], Windows XP [tm], includes a firewall that can be enabled for any external connection. There is little documentation about the XP [tm] firewall, because it is relatively new, though some initial reports indicate it does a good job of protecting the host computer from external scans. This may be in part because it is so new that adequate attack programs have not been developed for it yet.

Another increasingly popular product for broadband access protection is a small-scale router and hardware based firewall. These appliances provide varying degrees of protection with little or no connection performance loss. Routers will often provide, at a minimum, packet filtering based on source Internet Protocol (IP) addresses, dropping those packets that do not meet pre-determined rules set by the user. This could include packets that originate from an IP address, or range of addresses, that have been problematic in the past, or from the user's own IP address (which should not be the source of an external packet). Hardware based firewalls will also provide varying levels of inspection, but should at a minimum look at the header of the packet to protect against potential buffer overflow attacks, as well as to block packets from IP addresses set by the user.

Depending on the type of information being processed by the computer or the privacy concerns of the computer user, the use of encryption and secure deletion programs should be considered. Popular applications that accomplish these tasks are made again by McAfee[tm] and Symantec[tm]. The McAfee[tm] product is based on their purchase of PGP[tm], maker of the application by the same name. These products extend fingers into common production applications, as well as file managers, in order to provide their functionality with a minimum of hassle. For example, PGP[tm] will create a menu option that is in addition to standard menu options on a mail program. This option will contain all the commands necessary to encrypt an email message to another user, so long as that user's public encryption key is known. PGP[tm] also automates and simplifies the process of generating a user's public and private keys, as well as

managing the public keys of other users. PGP[tm] also creates a PGP[tm] menu option for file management that can be accessed by simply right-clicking a specific file. The PGP[tm] menu option will be available with the other standard options, and will provide functions such as encryption and secure deletion. Secure deletion is an important function because, as discussed earlier, Windows[tm] does not entirely delete a file when the delete key is pressed. Programs with secure delete functions accomplish full deletions by systematically deleting and overwriting affected sections of a hard drive numerous times.

When all else fails, a good backup system is critical. With the prevalence of large-volume rewritable media that can be obtained at relatively low cost, there really is not any excuse for not backing up. Both Zip[tm] Drives and rewritable CD drives make excellent backup mechanisms. There are commercial backup and recovery programs available that work quite well and are not necessarily very expensive. However, Windows[tm] will create a recovery disk for you, either during or after installation. Combined with original copies of licensed software and backups of critical data, the foundation of a good backup and recovery system is formed. Another benefit gained by the installation of a removable rewriteable media device is the ability to manage sensitive information, such as personal financial data, on media that can be removed from the computer. If this media is not present in it's associated device, even if a system is compromised (assuming all temporary files have been deleted), sensitive information is still protected. When considering the use of a backup system, remember that external forces, such as flooding or fire, can damage a personal computer just as readily as a malicious attack. In the event of one of these occurrences, the removable media that contains important personal financial information typically stored on a computer will be far easier to recover than a personal computer.

User Behavior

The single largest influence over a personal computer's susceptibility to attack is the computer's user. User behavior can affect every aspect of a personal computer's security, from patch currency, to anti-virus signatures, to what email attachments are opened. The social engineering of computer users is taken advantage of in a number of attacks. For example, email worms with titles such as "I Love You", "Anna Kournikova", and "My Party Pictures" are so named to entice users into opening them, even if the file extension is .vbs, or .exe. In addition, a quick way to install a trojan horse or a back door on another computer is to embed it in a program that would seem innocuous, harmless, or fun. Any executable program can be affected, including screen saver applications, games, or online chat programs that are often popular with average users. Even open-source technical vulnerability analysis programs used by security professionals must be thoroughly checked for trojan horses and back doors, especially since they are often collecting sensitive configuration or vulnerability information about networks and Web servers. The best defense against the spread of these types of malicious programs is to train users to avoid installing any application with an unidentifiable source. The same is true for opening email attachments. Users must be made aware that the integrity of no email attachment is beyond reproach, and

executable attachments in particular create a greater risk. In general, users should understand that executable attachments should never be opened without first verifying their authenticity by contacting the sender. When used as a part of a larger organization, this type of computer vulnerability can be mitigated by the institution of a policy addressing these types of actions, but this does not apply to home use.

Users should also be aware of their importance in protecting their personal computers, and how this extends to maintaining their computer's patch currency. During the Code Red and Nimda attacks, it was discovered that a number of personal computers running Windows 2000™ were particularly vulnerable because they were not as likely to ensure their systems were securely configured or had the same patch currency as enterprise servers. Also, these personal users were not as likely to be protected by a large firewall. Though patches correct or protect from technical vulnerabilities, the motivation to download and install a security patch is often a training and awareness issue, especially if strictly personal use of a computer removes any chance of having patch currency enforced by a policy. Similarly, this issue extends to the maintenance of anti-virus signatures. Though the use of an anti-virus program is a technical solution, the maintenance of the anti-virus signatures themselves is a user behavioral issue. Many new versions of popular anti-virus programs begin to address this by providing automatic update features.

Finally, as policies for creating stronger passwords with more frequent changes become more prevalent, it becomes more likely that users will cheat in organizational environments by writing their passwords down, or finding ways around no-reuse policies. This can translate into an absolute refusal to follow similar password policies for personal use. This can also be mitigated through the use of training and awareness programs, such as those that describe the use of password cracking programs. A policy requiring a complex password to be changed every 90 days may appear onerous to a typical user. However, the policy becomes far easier to understand with the demonstration of how quickly a password cracking program can break a weak password, as well as a demonstration of how long the same program will take to break a strong password.

The concept of defense in depth has been applied to large networks and major applications, and has gained greater understanding and implementation particularly over the past few years. This is increasingly driven by the propagation of threats accelerated by greater Internet connectivity and dependence. A failure to follow this approach on large enterprise-wide systems can lead to significant economic and credibility losses, as well as potential legal action related to due-diligence issues. However, the motivation for similarly protecting personal computers has not been as genuine. The increased use of broad band connections combined with the increased processing power and storage space of personal computers is changing this mindset. Now personal computers can be hijacked and used to attack other computers, or be the vulnerability for a connected network. Now personal computer security is being taken seriously.

Bibliography

Books

1. John Scambray, Stuart McClure, George Kurtz. Hacking Exposed Second Edition, Network Security Secrets and Solutions. Berkeley: The McGraw Hill Companies, 2001. 119-124, 433.

2. Michael A. Banks. PC Confidential. United States of America: Michael A. Banks, 2000. 94-96, 178-181, 192.

3. Aviel D. Rubin. White-Hat Security Arsenal, Tackling the Threats. United States of America: AT&T, 2001. 7-16, 69-75.

Web Pages

1. Salkever, Alex. "Broadband ISPs Shouldn't Knock Down Firewalls." Security Net. 20 November 2001. URL: http://www.businessweek.com/bwdaily/dnflash/nov2001/nf20011120_6165.htm. (12 January 2002).

2. Computer Emergency Response Team/Coordination Center. "CERT® Advisory CA-2001-19 "Code Red" Worm Exploiting Buffer Overflow In IIS Indexing Service DLL." 17 January 2002. URL: http://www.cert.org/advisories/CA-2001-19.html. (28 January 2002).

3. Computer Emergency Response Team/Coordination Center. "CERT® Advisory CA-2001-26 Nimda Worm." 25 September 2001. URL: http://www.cert.org/advisories/CA-2001-26.html. (25 September 2001).

4. Hopper, Ian D. "Hacked @ home." URL: http://www.rockymountainnews.com/dmn/technology/article/0,1299,DRMN_49_929462,00.html. (28 January 2002).

5. Thorsberg, Frank. "Is your PC open to attack?" CNN.com/SCI-TECH. 17 May 2001. URL: http://www.cnn.com/2001/TECH/internet/05/17/zombies.idg/index.html. (21 January 2002).

6. Bruce, Ian S. "It's time to arm your system to combat cyber war." 21 October 2001. URL: http://www.sundayherald.com/print19370. (7 January 2002).

7. Strom, David. "Let's Talk About Passwords." Ecommerce In Action. 31 October 2001. URL: http://www.itworld.com/nl/ecom_in_act/10312001/?idgnet. (5 January 2002).

8. Microsoft. "Microsoft Office XP Security White Paper." Technical Resources> Administration & Interoperability. March 2001. URL: http://www.microsoft.com/Office/techinfo/administration/security.htm. (28 January 2002).

9. Pruitt, Scarlet. "Survey: Net shoppers stay home in November." CNN.com/SCI-TECH. December 11, 2001. URL: http://www.cnn.com/2001/TECH/industry/12/11/net.shopping.idg/index.html. (17 January 2002).

10. National Infrastructure Protection Center. "Trust But Verify: A Guide to Using E-Mail Correspondence." December 2001. URL: http://www.nipc.gov/publications/nipcpub/penpals.html. (5 January 2002).

11. Zaborav, Dev. "Understanding Password Cracking." Unix Security. 13 December 2001. URL: http://www.itworld.com/nl/unix_sec/12132001/?idgnet. (5 January 2002).

12. Greene, Thomas C. "Win-XP firewall defeats Gibson NanoProbes." 26 October 2001. URL: http://theregister.co.uk/content/55/22509.html. (10 January 2002).

Other Publications

1. Marrianne Swanson, Barbara Guttman. NIST Special Publication 800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems. September 1996. Washington, D.C. National Institute of Standards and Technology, Technology Administration, United States Department of Commerce.