CERT-In Security Guideline CISG-2005-03

CERT-In

Indian Computer Emergency Response Team

Enhancing Cyber Security in India

SECURING HOME COMPUTERS

Department of Information Technology
Ministry of Communications and Information Technology
Govt. of India

Issue Date: 31-12-2005

INDEX

1. Introduction

This document is intended to prescribe basic guidelines to the home computer users working with computer systems running Windows Operating System**.** The basic purpose of this document is to create awareness about computer security issues among home computer users and suggest them the tasks to be performed to secure their computer systems to protect their information assets.

1.1 Why Home Computers?

Home computers are typically not very secure and are easy to break-in. When combined with high-speed Internet connections that are always turned on, intruders can quickly find and then attack home computers. While intruders also attack home computers connected to the Internet through dial-in connections, high-speed connections (cable modems and DSL modems) are a favorite target. There may not be important data stored on the home computers but they are targeted by the intruders for launching attack against other computer systems.

1.2 How attackers do it?

In general, attack vectors which attackers use are:

- Through E-mail
- Through Un-trusted Websites
- Through Internet Shares

In some cases, they send email with a virus. Reading that email activates the virus, creating an opening that intruders use to enter or access the computer. In other cases, they take advantage of a flaw or weakness in one of the computer program’s vulnerability – to gain access. Once they’re on the computer, they often install new programs that let them continue to use the computer – even after user plug the holes they used to get onto user’s computer in the first place. These are known as “backdoors” and are usually cleverly disguised so that they blend in with the other programs running on user’s computer.

In general, they steal the information saved by the user on his system or use the system to launch attack on other computer systems.

1.3 What is Information Security?

Information security can be explained by the help of following example. If company sells bottled water purified using the process of reverse osmosis, the process is well known, and therefore it does not make good business sense for management to protect that information. However, if that company has a revolutionary process that cuts the cost and time for water purification in half, it would make sense to secure that information. There is a limit to the value of implementing protection so user must combine his knowledge of value, threats, vulnerabilities, and risks to put together a feasible plan.

Information security involves the measures and controls that ensure confidentiality, integrity, and availability of the information processed by and stored in a computer or system.

Confidentiality: *Ensures that information is accessed only by authorized personnel.*

Integrity: *Ensures that information is modified only by authorized personnel.*

Availability: *Ensures that information and systems can be accessed when needed by authorized personnel.*

This practice include policies, procedures, hardware and software tools necessary to protect the computer systems and the information processed, stored, and transmitted by the systems.

When the user combines efforts to provide data confidentiality, data integrity, and data availability with physical security, then he can provide a very effective security solution.

1.4 Threats to the home computers

A threat, for information security, is any activity that represents possible danger to user's information.

Intruders want the information stored by the users which are personal and sensitive, such as credit card numbers, PINs, passwords etc. By stealing this information the malicious intruders commonly referred to hackers may gain financially. The intruders also use the resources of the compromised systems for their own purposes and for attacking other computer systems connected to the Internet. Recent trends in computer security threats show that the attackers are compromising the home computers and installing malicious code such as Bots in these systems, which may then be used as Zombies to further launch large scale attacks on critical information systems. This type of attack is known as Distributed Denial of Service (DDOS).

1.5 Vulnerabilities in home computer

A vulnerability is a weakness in user's information security that could be exploited by a threat; that is, a weakness in user's system and network security, processes, and procedures.

Computer vulnerability is flaw in the computer system. Which when exploited allows intruder to compromise the system's integrity. The common types of vulnerabilities are logical errors in operating system or applications due to poor coding techniques, allowing intruder to exploit them and giving him heightened access to the user's computer. Various security tools are available to secure the system like firewalls etc. These tools provide excellent security mechanism but having flaw in design that could lead to security breach. The term "security through obscurity" fits into this arena, being the system is secure because nobody can see hidden elements. All types of file encryption come under this category. By means of encrypting the data an additional layer of protection is being added to the computer system. In case a system is compromised, the critical data is still protected by encryption. And the intruder may not be able to steal the information from the hacked system.

1.6 What is Intrusion?

The users of home computers normally connect to internet through dial-in modems or internet connection through cable. Intruders are always looking for new ways to break into computers connected to internet. They may attempt to breach the computer security defenses from remote locations. Intruders seek old, unpatched vulnerabilities as well as newly discovered vulnerabilities in operating systems, network services, or protocols[1] and take advantage of each. They develop and use sophisticated automated programs to rapidly penetrate the systems, alive on the Internet. Once the attacker is able to find a vulnerable system, he exploits the system to steal information or to launch further attacks.

1.7 Malicious Code

Malicious code, or malware, is a common name applied to all forms of unwanted and destructive software, such as viruses, worms, and Trojans. The best way to protect from malicious code is to install virus scanners and keep virus definition[2] (signature) files current.

Virus: *A virus is malicious code that infects or attaches itself to other objects or programs. All viruses have some form of replication mechanism, which is how they propagate.*

Worm: *A worm is malicious code that replicates by making copies of itself on the same computer or by sending copies of itself to another computer. Worms, unlike viruses, do not infect other program files on a computer. All worms have some form of replication mechanism, which is how they propagate. A worm does not require any host program unlike virus to execute, they can run independently.*

Trojan: *A Trojan horse is seemingly useful (or harmless) programs that perform malicious or illicit action when activated, such as destroying files. For example, user downloads what appears to be a movie or music file but he unleash a*

[1] A Protocol is a set of language by which two computers talk to each other.

[2] Virus Definition is the identity of a known virus.

dangerous program which can erase in disk or can send his credit card numbers or password files to intruders.These backdoor programs may also open certain ports on user computer allowing unauthorised access to user computer.

The malicious code usually propagates through email attachments.

1.8 Key loggers

Key loggers are software application (or hardware based as well) which are able to capture the key logging events and can mail them to remote intruder via email. These are invisible and undetectable to users so there is a huge risk of sending important information such as credit card numbers passwords to the remote intruders. The set program can be combined with useful applications like that whenever user install that application the key logger program also get installed along with that application.

1.9 Bots

The term Bot is derived from the word “Robot”. Robot comes from the Czech word "robot," which means "worker". In computer world Bot is a generic term used to describe an automated process.

Bots are being used widely on the Internet for various purposes. Bot functionality may vary from search engines to game bots and IRC channel bots. Google bot is one such famous search bot, which crawls through the web pages on the net to collect information and build database to enable variety of searches. Computer controlled opponents and enemies in multiple player video games are also a kind of bot, where the computer process tries to emulate the human behavior.

However, the usage of bots is not limited to good purpose only. Bots are widely used to perform malicious activities ranging from information stealing to using as a launching pad for distributed attack. Such software’s gets installed on user’s computer without their knowledge. Some bot infected machines, pass the control of the machine to a remote attacker and act as per the attackers command. Such machines are popularly known as zombie machines.

CERT-In has published a white paper on Botnet: An Overview which gives in-depth details on botnets.

1.10 Adware and Spyware

Adware is 'freeware', whereby ads are embedded in the program. These ads will show up whenever user opens the program. Most adware authors provide the free version with ads and a registered version whereby the ads are disabled.

As such, the users have the choice, either to use the freeware with ads served or purchase the registered version.

Spyware, as the name suggest is the software installed on user’s computer which is constantly sending user information to the mother website.

Spyware, however, is published as 'freeware' or as 'adware', but the fact that an analysis and tracking program (the 'spyware' agent, which reports user’s activities to the advertising providers' web site for storage and analysis) is also installed on user’s system when a user install this so-called 'freeware', and this is usually not mentioned. Even though the name may indicate so, spyware is not an illegal type of software. But what the adware and spyware providers do with the collected information and what they're going to 'feed' the user with, is beyond his control. And in some cases it all happens without the user’s consent.

For a comprehensive list of spywares, please refer:
http://www.spywareguide.com

1.11 Indications of Infection

Some of the indications are given below:

- Poor system performance
- Abnormal system behavior e.g. system restarts or hangs frequently.
- Unknown services are running
- Crashing of applications
- Change in file extensions or contents
- Hard Disk is busy or its light glows continuously

Since we have discussed the basic terminologies and methodologies, now we can start discussing the defensive actions.

2. Securing home computers with Defense in depth strategy

To ensure that the information is secured during process, storage and transmission certain security measures are to be taken by the users of that information.

Following sections will describe certain tasks that are to be performed by the user to secure the computer systems being used at home and information stored or processed therein.

These tasks broadly involve steps to prevent computer security incidents.

2.1 The Defense in Depth Approach for the Home User

A defense in depth strategy is the traditional one adopted to afford the defended area the strongest and most resilient protection. In the case of the home Internet user, the defended area is the user’s data. As shown in Figure 1, defense in depth for the home user consists of defensive measures adopted in four layers, namely: network access; the operating system; user applications; and data. At the center of the defended area is the most valued component of the defended area – the user’s data.

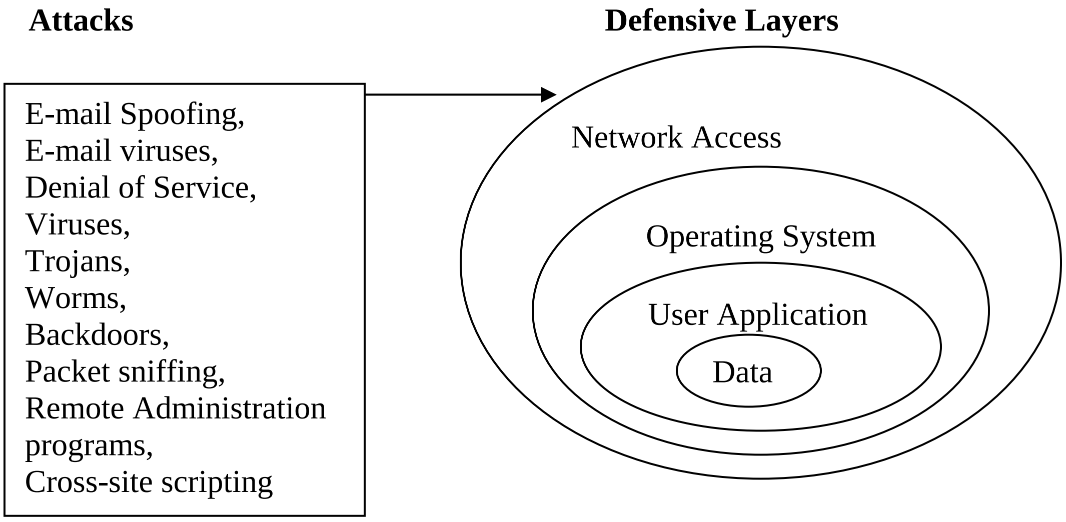


Figure-1: Most common Intruder methods used against home computers

This layered approach is required since even the most expensive firewall controlling network access cannot effectively control traffic content. For example, most firewalls will allow an e-mail attachment containing viruses. These viruses may be cleaned at the operating system layer by anti-virus software if they are recognized. However, if they are of an unknown type, then the final defense is at the data layer where the user opens the e-mail attachment with care. Apart from this, user data is protected by means of rights & privileges and encryption techniques.

To be effective, defensive measures at each layer must be based on the threats to the defended area. The recommended defensive measures at each layer of the defense vary as shown in Table 1.

Of course home user should consult their system support personnel for advice.

1.5 Defensive Measures

Table-1: Defense in Depth – Defensive Actions at each layer

Defensive Layer	Defensive Measures	Remarks
Network Access	Use a Firewall	Hardware or Software Firewall
	Disconnect from the Internet when not using it	User Training
Operating System	Keep up-to-date security patches and update releases for Operating System	Ongoing Activity
	Make a boot/ERD disk and keep it current	Ongoing Activity
	Install and keep up to date Anti virus software	Ongoing Activity
	Install and keep up to date AntiSpyware software	Ongoing Activity
	Harden OS by turning off unnecessary clients, services and features	One time Activity
User Application	Keep up-to-date security patches and update releases for application software	Ongoing Activity
	Don’t install programs of unknown origin	Ongoing Activity
	Precautions with E-mail	Ongoing Activity
	Protection from Phishing attacks	Ongoing Activity
	Chat Clients	Ongoing Activity
	Securing Web Browser	One Time Activity
Data	Backup Important files	Ongoing Activity
	Use encryption to ensure confidentiality of sensitive data	User Training
	File Checksum	User Training
	Password Policy	User Training
	Login Settings	User Training
	Audit Policy Settings	User Training
	Event Viewer	Ongoing Activity

The defensive actions have been identified at each layer, it is necessary to discuss how these actions will be carried out for a Windows-based home Internet user. It is also important to keep in mind that the defensive posture is weakened when one does not implement the entire defense in depth strategy that is being advocated. For example, using a firewall but having either no or outdated antivirus software, leaves the system vulnerable.

3. Defensive Measures at Network Access Layer

This is the first layer of the defense in depth model. The defensive measures that have to be taken at this layer are:

- Use a Firewall.
- Disconnect from the Internet when not using it.

3.1 Use a Firewall

A firewall places a virtual barrier between the computer and hackers, who might seek to delete information from the computer, make it crash, or even steal personal information.

The firewall serves as the primary defense against a variety of computer worms that are transmitted over the network. It helps to protect the computer by hiding it from external users and preventing unauthorized connections to the computer.

For home users, a firewall typically takes one of two forms:

- Personal firewall - specialized software running on an individual computer, e.g. ZoneAlarm and in-built Windows Internet Connection Firewall (ICF) etc.
- Hardware firewall - a separate device designed to protect one or more computers, e.g. Linksys EtherFast Cable/DSL Router.

If user is having a home network, it is recommended that he should have both types of firewall installed i.e. hardware firewall at the router[3] and personal firewall at each system using that network. But if the user is using a stand-alone PC only, then it is recommended that he should have at least a personal firewall installed on the PC.

3.1.1 Installing Personal Firewalls

A Personal firewall or desktop firewall is a software program that provides primary defense mechanism for the desktop computer connected to the internet.

The firewall acts like a guard, who checks everybody entering or going out of the home and based on some prior knowledge allows or disallows the people.

Once the personal firewall is being installed, it is continuously running in the background, watching out all the incoming and outgoing traffic. Simultaneously it reports to the user by giving a pop-up about the program which is trying to access the internet or conversely trying to access the user’s system. It is solely the discretion of the user that to whom or which program he wants to allow through the firewall.

[3] Hardware that helps LANs and WANs achieve interoperability and connectivity.

Users should be exceptionally careful when allowing a particular program or file through the firewall. And have to be very considerate about which file is used by which particular program.

3.1.2 Why firewall is needed?

If the computer is not protected when the user connects to the Internet, hackers can gain access to personal information from the computer. They can install code on the computer that destroys files or causes malfunctions. They can also use user's computer to cause problems on other home and business computers connected to the Internet. A firewall helps to screen out many kinds of malicious Internet traffic before it reaches to the user's system.

Some firewalls can also help to prevent others from using user's computer to attack other computers without user's knowledge. Using a firewall is important no matter how the user connects to the Internet — dial-up modem, cable modem, or digital subscriber line (DSL or ADSL).

Microsoft Corporation provides Internet Connection Firewall for Windows XP SP2 users only. For the users running old versions of Windows (9x, NT or 2000), they have to select a desktop firewall according to their needs from third party. While Windows 2000 does not having a purpose-built firewall, it does have IP Security filters that can be used to make a static packet filter.

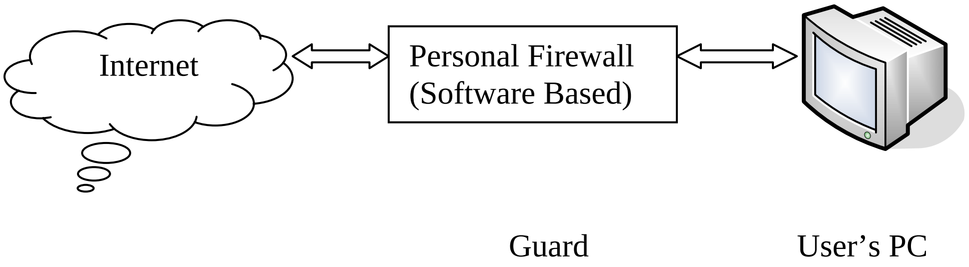


Figure-2: Protecting the Internet-connected Home PC

Figure 2 shows where the personal firewall fits into the connection of a home PC to the Internet. Obviously the personal firewall is not a discrete component, rather it is software that runs on the home PC, but it's shown separately for clarity. As illustrated, the goal of the personal firewall is to ensure that traffic from intruders cannot reach the home PC – understanding that the firewall will not block attachments bearing malicious code.

Some of the shareware firewalls are listed below:

http://www.free-firewall.org/

http://www.zonelabs.com

http://smb.sygate.com/download_buy.htm

http://www.iopus.com/guides/free-firewall.htm

http://www.firewallguide.com/freeware.htm

3.1.3 Configuring Internet Connection Firewall

Windows XP with SP2 includes a built-in firewall called the Internet Connection Firewall (ICF). By default it is disabled, ICF can provide an additional layer of protection against network based attacks such as worms and denial-of-service (DoS) attacks. To Enable ICF do the following steps:

1. Go to **Start menu\Control Panel\Network and Internet Connections\Network Connections**\ Under the **Dial-Up** or **LAN or High Speed Internet** category, click the icon to select the connection that user wants to help protect.

2. In the task pane on the left, under **Network Tasks**, click **Change settings of this Connection** (or right-click the connection user wants to protect, and then click **Properties.**

3. On the **Advanced** tab, under **Internet Connection Firewall**, check the box next to **Protect my computer and network by limiting or preventing access to this Computer from the Internet**.

There are some limitations with ICF that must consider before enabling it. ICF does not have the rich feature set provided by many third party products. This is because ICF is intended only as a basic intrusion prevention feature. ICF prevents people from gathering data about the PC and blocks unsolicited connection attempts. The biggest limitation of ICF is that it protects the user only from inbound pests; it doesn't alert the user to suspicious outbound traffic.

3.2 Disconnect from the Internet when not using it

The user relying on traditional dial-up access to the Internet will likely disconnect when they are not using the connection since usage limits apply and they may only have one phone line. On the other hand, home users with "always-on" broadband access services such as cable modems or DSL/ADSL+ may be tempted to leave their computer permanently connected to the Internet. A permanent connection allows them to access their files over the Internet from a remote location. The problem is that the longer one remains connected, the longer an intruder gets time to attack the host.

It is recommended for the broadband home users that they should turn-off their cable/DSL/ADSL modems when they are not using Internet at all.

Or for those users who are directly connected to their ISP with their network cards, they should disable their network cards in the operating system when they are not using their systems to access internet

To disable the network card in Windows 98, follow the following steps:

Right-click My computer\select properties\ click device manager

Expand Network Adapters

Select the Network adapter that is used for ISP connection

Click properties

Select Disable in this hardware profile.

To disable the network card in Windows 2000/XP, follow the following steps:

Right-click My network places\ select properties

Select the Local Area Connection used for connecting ISP.

Right-click and select Disable.

4. Defensive Measures at Operating System Layer

This is the second layer of the defense in depth model. The defensive measures that have to be taken at this layer are:

- Keep up-to-date security patches and update releases for Operating System.
- Make a boot/ERD disk and keep it current
- Install and keep updated Antivirus software
- Install and keep updated Antispyware software
- Harden Operating System by turning off unnecessary services and features

4.1 Keep up-to-date security patches and update releases for Operating System

The most important program that runs on a computer is Operating System. Every general-purpose computer must have an Operating System to run other programs. Operating System perform basic tasks, such as recognizing input from the keyboard, sending output to the monitor, keeping track of files and folders on the disk and controlling peripheral devices such as disk drives and printers. Some of the common Desktop Operating Systems are Windows (9x, NT Workstation, 2000 Professional, XP Home Edition & Professional Edition) and Linux workstation etc.

Application software sits on top of Operating system because it is unable to run without the Operating System. Application software (also called *end-user programs*) includes word processor like MS Word, databases like SQL or Oracle etc.

It is the most essential task that every user has to do as it is repetitive ongoing activity. Every time vulnerability is explored the vendors releases the respective patch and that has to be installed immediately after release. If not, that might be an open door to exploit the system.

The user should subscribe the security newsletter from the respective vendors, whose software he is using. Accordingly, whenever a security patch or a hotfix[4] *is being released the user will be intimated and can act accordingly.*

Now days, the every application has the feature to update automatically through Internet. The user should cautiously configure the respective applications.

[4] A Patch or Hotfix is a small program released by the vendor which fixes up the software for known bugs and vulnerabilities.

4.1.1 Using "Windows Update"

"Windows Update" is a Microsoft Web site that provides updates for Windows operating system software and Windows-based hardware. Updates address known issues and help protect against known security threats. The patches, hot fixes and service packs released by the Microsoft Corporation are free of cost.

When any user visit the Windows Update Web site i.e. http://www.windowsupdate.com , Windows Update scans the user's computer and tells which updates are missing and should be applied to his system. The user chooses the updates that he wants to install and how to install them.

"Windows Update" uses the following categories:

- **High priority:** Critical updates, security updates, service packs, and update rollups that should be installed as soon as they become available and before user install any other updates.
- **Software (optional):** Non-critical fixes for Windows programs, such as Windows Media® Player and Windows Journal Viewer 1.5.
- **Hardware (optional):** Non-critical fixes for drivers and other hardware devices, such as video cards, sound cards, scanners, printers, and cameras.

Optional updates address minor issues or add non-critical functionality to user's computer. It is more important to install high priority updates so that the user's computer gets the latest critical and security-related software.

4.1.2 Difference between Express and Custom Windows Update?

- **Express (recommended)** displays all high priority updates for user's computer so that he can install them with one click. This is the quickest and easiest way to keep user's computer up to date.
- **Custom** displays high priority and optional updates for user's computer. User must review and select the updates that he wants to install, one by one.

4.1.3 Automatic Updates

Automatic Update is a feature that works with Windows Update to deliver critical and security-related updates as they become available. When the user turns on Automatic Updates (recommended), Windows automatically looks for high priority updates for user's computer. Windows recognizes when the user is online and uses the Internet connection to search for downloads from the Windows Update Web site. An icon appears in the system tray each time new updates are available.

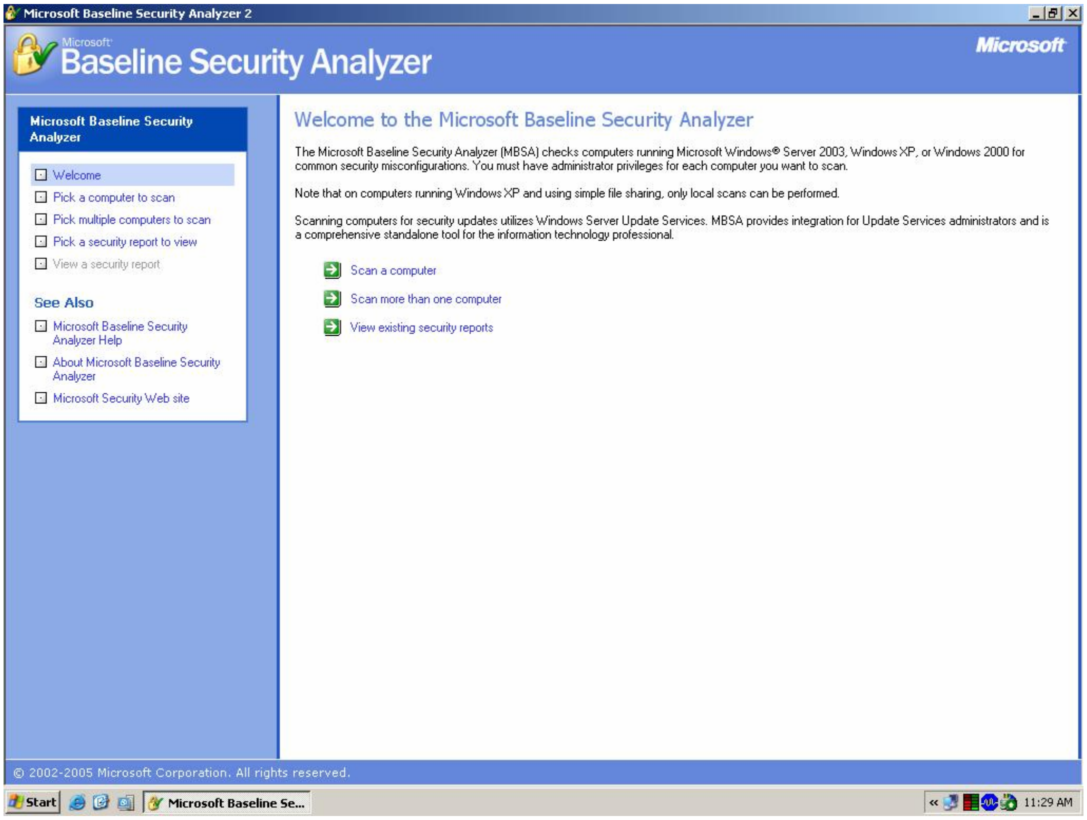
Users have to decide how and when the updates are installed. Sometimes, some updates require the user to accept an End User License Agreement (EULA), answer a question about the installation process, or restart the computer before the user can install them.

Automatic Updates delivers only high priority updates. To get optional updates, the user still needs to visit the Windows Update Web site.

Microsoft releases Windows patch on the second Tuesday of each month, so to be safe, checks for the updates manually every couple of weeks. As there may be a lag between when a patch is available and when Windows Update pushes it to the user's system (as the system has been off for more than a few days).

4.1.4 Using MBSA

MBSA is Microsoft Baseline Security Analyzer version 2.0 gives the ability to assess the administrative vulnerabilities present on one or multiple systems. MBSA scans the specified computers and then generates a report that contains details for each computer about the security checks that MBSA performed, the results, and recommendations for fixing any problems. In addition to checking for misconfiguration that might cause security problems in the operating system, user can check for security problems in Microsoft SQL Server and Microsoft Internet Information Services (IIS). User can also determine whether a computer has the most current Microsoft Windows and Microsoft Office updates installed, and can check for security updates, update rollups, and service packs for other products hosted by the Windows Update site.


Microsoft Baseline Security Analyzer 2
Microsoft
Baseline Security Analyzer
Microsoft
Microsoft Baseline Security Analyzer
Welcome
Pick a computer to scan
Pick multiple computers to scan
Pick a security report to view
View a security report
See Also
Microsoft Baseline Security Analyzer Help
About Microsoft Baseline Security Analyzer
Microsoft Security Web site
Scan a computer
Scan more than one computer
View existing security reports
Start
Microsoft Baseline Se...
11:29 AM

Welcome to the Microsoft Baseline Security Analyzer

The Microsoft Baseline Security Analyzer (MBSA) checks computers running Microsoft Windows® Server 2003, Windows XP, or Windows 2000 for common security misconfigurations. You must have administrator privileges for each computer you want to scan.

Note that on computers running Windows XP and using simple file sharing, only local scans can be performed.

Scanning computers for security updates utilizes Windows Server Update Services. MBSA provides integration for Update Services administrators and is a comprehensive standalone tool for the information technology professional.

© 2002-2005 Microsoft Corporation. All rights reserved.

MBSA comes in two flavors: GUI tool and command line tool. Users can get more details about MBSA from the following URL:

http://www.microsoft.com/technet/security/tools/mbsahome.mspx

User should be connected to the Internet while running MBSA for the first time.

4.2 Make a boot/ERD disk and keep it current

A boot disk allows the user to boot from a diskette instead of the hard drive. This can prove useful in accessing the system in the event of either a security incident or hard disk failure. It must be done before an incident requiring its use arises. In Windows 9x,

- Go to Start\Settings\Control Panel\Add or Remove programs.
- In Add or Remove Programs window, click on the tab Startup Disk, click on tab create now.

Some versions of Windows, e.g. Windows NT, Windows 2000 and Windows XP can use the emergency repair procedure to fix problems that may be preventing the computer from starting. However, using the emergency repair procedure to fix the system generally requires an existing Emergency Repair Disk (ERD). This disk should be regularly updated and stored in a safe place.

An ERD is created differently depending on the version of Windows. The Backup utility in both Windows 2000 and Windows XP is used to create an ERD; while in Windows NT the “rdisk /s” command is used.

As a general practice, the ERD should be made immediately after the installation of operating system. And should be updated whenever any security update is applied or any configuration of operating system is being changed.

4.3 Install and keep up-to-date Antivirus Software

Anti Virus software look at the contents of each file, search for specific patterns that match a profile – called a virus signature – of something known to be harmful. For each file that matches a signature, the anti-virus program typically provides several options on how to respond, such as removing the offending patterns or destroying the file.

Viruses can reach the computer in many different ways, through floppy disks, CD-ROMS, email, web sites, and downloaded files. It needs to be checked for viruses each time before using any of them. Anti-virus program do these automatically, if configured properly. Anti-virus vendors provides regular update for these virus signatures, because everyday many new viruses are discovered and released, making the system prone to virus attacks and without an antivirus update, antivirus is ineffective against such attacks.

The anti-virus software should include features such as the automatic updating of its virus definition files, scanning and cleaning of both incoming and outgoing email messages, script blocking and real-time anti-virus protection.

Installing an anti-virus program and keeping it up-to-date is among the best defenses for home computer and offers the effective protection against computer viruses.

These are some of the freeware antivirus software available on internet

www.grisoft.com/us/us_dwnl_**free**.php

www.free-av.com/

www.pandasoftware.com/activescan/

www.avast.com/eng/down_home.html

www.freebyte.com/antivirus/

CERT-In has published a guideline on “Anti Virus Policy & Best Practices” which gives the in-depth details of using Anti-virus software

4.4 Install and keep up-to-date AntiSpyware Software

AntiSpyware software helps to protect users from spyware and other potentially unwanted software like adware. AntiSpyware helps to reduce negative effects caused by spyware, including slow computer performance, annoying pop-up ads, unwanted changes to Internet settings, and unauthorized use of user's private information. Continuous protection improves Internet browsing safety by guarding spyware in ways they can enter the system. The worldwide SpyNet community plays a key role in determining which suspicious programs are classified as spyware.

AntiSpyware gives the real-time protection by monitoring the system at different checkpoints. These checkpoints are triggered when programs make changes to Windows configuration. These changes can occur when user installs software on his system, or they can occur when spyware or other potentially unwanted software attempts to install on the system.

In case Real-Time Protection detects a change in any checkpoint, AntiSpyware alerts the user and provides the option for user to allow or block the change.

A good AntiSpyware gives the real-time protection, the counteract methods and updates itself for the latest checkpoints & spyware.

Different AntiSpywares are available on the Internet. Microsoft has also released an antispyware by the name **Microsoft AntiSpyware (Beta)**, which is available free on its site. For more details on Microsoft AntiSpyware (Beta), refer to the following link:

http://www.microsoft.com/athome/security/spyware/software/default.mspx

4.5 Harden the Operating System by turning off unnecessary clients, services and features

Hardening of the operating system (OS) is a topic on its own for which there are a number of good references releases time to time on product basis by their respective vendors. Discussion on hardening on Operating System is beyond the scope of this document. For further reading on hardening the Operating System, please see the following links:

http://www.microsoft.com/downloads/details.aspx?FamilyId=2D3E25BC-F434-4CC6-A5A7-09A8A229F118&displaylang=en

a. Turn off the "Hide file extensions for known file types" feature:

By default, Windows hides the file extensions of known file types. This behaviour has been used to trick users into executing malicious code. But a user may choose to disable this option in order to have file extensions displayed by Windows. Multiple email-borne viruses are known to exploit hidden file extensions. The first major attack that took advantage of a hidden file extension was the VBS/LoveLetter worm which contained an email attachment named "LOVE-LETTER-FOR-YOU.TXT.vbs". Other malicious programs have since incorporated similar naming schemes, examples include:

- Downloader (MySis.avi.exe or QuickFlick.mpg.exe)
- VBS/Timofonica (TIMOFONICA.TXT.vbs)
- VBS/CoolNote (COOL_NOTEPAD_DEMO.TXT.vbs)
- VBS/OnTheFly (AnnaKournikova.jpg.vbs)

The files attached to the email messages sent by these viruses may appear to be harmless text (.txt), MPEG (.mpg), AVI (.avi) or other file types when in fact the file is a malicious script or executable (.vbs or .exe, for example).

For further information about these and other viruses, visit the following link.

http://www.cert.org/other_sources/viruses.html

b. Remove the ability of others to access file shares and printers on the host since poorly protected file shares are being actively targeted:

For all Windows users:

- Disable by deselecting the "File and Printer Sharing for Microsoft Networks" option in the Network and Dial-Up Connections applet. This service allows networked computers to transparently access files that reside on remote systems.
- Disable by deselecting the "Client for Microsoft Networks" option in the Network and Dial-Up Connections applet. This service will disable the facility that allows a distributed application to call services that are available on various computers on a network.

For Windows 2000 and XP users only:

To enable or disable the services in aforesaid Operating Systems go to Start>Settings>Control Panel>Performance and Maintenance>Administrative Tools>Services:

- Disable Performance Logs & Alerts: This service collects performance data from local or remote computers based on preconfigured schedule parameters.
- Disable Remote Registry Service: This service enables remote users to modify registry settings on local computer.

- Disable Windows Management Instrumentation (WMI) Driver Extensions: This service provides systems management information to and from drivers.
- Disable TCP/IP NetBIOS Helper Service: This service enables name resolution over TCP/IP.
- Disable Remote Administration Service: This service provide total control of user's system to the remote user. (To disable this service, right click on My Computer>Properties>Remote Tab, then deselect "Allow Remote Assistance invitations to be sent from this computer")

Users should be extremely cautious about disabling the above mentioned services, as it is quiet possible that they might be using these services for different purposes in their environment. Disabling these services before any consent could result in malfunctioning of program/s. Please consult to the system vendor before taking any step.

5. Defensive Measures at User Application Layer

This is the third layer of the defense in depth model. The defensive measures that have to be taken at this layer are:

- Keep up-to-date security patches and update releases for Application software.
- Do not install programs from unknown origin
- Precautions with E-mail
- Chat clients
- Securing Web browser

5.1 Keep up-to-date security patch and update releases for Application Software

Just as new vulnerabilities appear regularly in the Operating System, so too they also appear in applications. Hence keeping applications patched is important.

In general, the announcement of new product vulnerabilities can be monitored by subscribing to one or more of the e-mail based free security alerting services. These services describe the latest vulnerabilities and generally indicate either how to get the required patch or the workaround pending a patch release.

5.2 Do not install programs of unknown origin

Installing programs of unknown origin exposes the user to the possibility of running malicious code. In general, programs to be installed should have been authored by company that is trusted and the download site should be a similarly trusted source.

Virus scanning of any such program prior to installation is always recommended. It is also recommended that user should not use pirated software's, as these pirated software's might install some kind of backdoors which can be used to hack the system as and when the hacker wants.

5.3 Precautions with Email

In general a user receives lots of e-mails every day, most of which are unsolicited and contains unfamiliar but believable return addresses.

5.3.1 Email spoofing

Email “spoofing” is when an email message appears to have originated from one source when it actually was sent from another source. Email spoofing is often an attempt to trick the user into making a damaging statement or releasing sensitive information (such as passwords).

Spoofed email can range from harmless pranks to social engineering ploys. Examples of the later include:

- email claiming to be from a system administrator requesting users to change their passwords to a specified string and threatening to suspend their account if they do not comply
- email claiming to be from a person in authority requesting users to send them a copy of a password file or other sensitive information
- Mail uses social engineering to tell the user of a contest that the user may have won or the details of a product that the user might like. The sender is trying to encourage the user to open the letter, read its contents, and interact with them in some way that is financially beneficial – to them.

5.3.2 Protection from spam

Spam is flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it. Most spam is commercial advertising, often for dubious products or get-rich-quick schemes. Spam costs the sender very little to send -- most of the costs are paid for by the recipient or the carriers rather than by the sender.

CERT-In has published a white paper on “An Overview of SPAM: Impact and Countermeasures” which gives in-depth details on spam.

5.3.3 Never respond to spam

Most of spammers say in their mail to unsubscribe click here but they’re lying. What they really want to do is confirm that they’ve got a live address. Also, if the user respond, they’ll sell their addresses to every other spammer meaning user soon be flooded with even more spam.

5.3.4 User should not post his address on his website

It seems like a good idea at the time, but posting an email address on a personal home page is just an invitation to spammers. Spammers and the people who sell spamming as a business have software that "harvests" email addresses from the Net. This software crawls through the Internet seeking text strings that are -something-@-something-.-something-. When it finds one, it catalogs it on a database of other email addresses to be used to send spam.

It is recommended that instead of giving e-mail in text form at the website, user should give an image of it.

5.3.5 Use a second email address in newsgroups

Newsgroups are the great email address gathering ground for spammers. If someone posts to a group, he is going to get spam -- it is just a matter of time. So how is he supposed to participate? Use a different email address for talking to friends and relatives. In other words, have a public address and a private address. One has to deal with spam only on his public address.

5.3.6 User should not give his email address without knowing how it will be used

If a website is asking for email address, they want to use it for something. Be sure to know what. Read the terms of use and privacy statements of any site before telling them email addresses, if there is not any privacy statement; don't tell them email address.

5.3.7 Use a spam filter

While there is no such thing as a perfect filter, anti-spam software can help keep spam at manageable level. Some of it is cumbersome, some works better than others, some even requires that the user let his email messages go through another system for storage and cleaning.

5.3.8 Never buy anything advertised in spam

The reason that people spam is because they can make money. They make money, like all advertisers, by convincing people to buy a product. If no one buys the things advertised in spam, companies will quit paying spammers to advertise their products.

5.3.9 Disable scripting features in e-mail programs when possible

Since e-mail programs frequently use the same code as web browsers to display HTML formatted messages, the vulnerabilities that affect ActiveX, Java, and JavaScript are often applicable to e-mail. Apart from disabling these features, the ability to run Visual Basic Scripting (VBS) should be removed if possible.

Viruses such as ILOVEYOU contain attachments ending in .vbs which infect the host when user clicks on the attachment to open it.

5.4 Protection from Phising attacks

When user receives an e-mail asking him to visit his bank’s web site, it signifies the beginning of a phishing fraud. The e-mail would usually provide a link to bank’s web site and ask the user to click the link. It would ask him to provide certain confidential banking information like his account number, credit card number etc., failing which his account would be doomed. There would be a sense of urgency and panic in the e-mail. This type of attack is called as phising attack.

Here is a checklist which helps to prevent this type of attack

- Check to see if the e-mail is indeed from the user’s bank and not from just any bank. If it isn’t, stop reading further and confirm the same from the by using other means like telephone.
- If the e-mail is not personally addressed to the user, it is most probably a fraud.
- Check the language and spelling of the text contained in the e-mail. If the user find misspelled words or substandard language, conclude that it is not from his bank
- If the e-mail urges the user to act immediately without delay, failing which his account will be closed down, stop reading it. It is not from user’s bank.
- If there is anything that even remotely feels wrong, stop. If something feels wrong, it is most probably wrong.
- Never click any link given inside the e-mail message. Instead, directly type the URL of the financial institution.
- If the user does not know the URL of his bank’s web site, take the time to call them immediately to find out.
- User should never provide personal information to anybody, come what may.

CERT-In has published a white paper on “Phishing Attacks and Countermeasures” which gives in-depth details on phishing.

5.5 Do not visit untrusted websites

It is always recommended that the user should not visit the untrusted websites or download software’s, screensavers or games etc from those untrusted sites. There is a possibility that these types of application software install some kind of malicious code on the user’s system, which can be used to launch attack on other computer systems without any consent of the user.

5.6 Chat clients

Internet chat applications, such as instant messaging applications and Internet Relay Chat (IRC) networks, provide a mechanism for information to be transmitted bi-directionally between computers on the Internet. Chat clients provide groups of individuals with the means to exchange dialog, web URLs, and in many cases, files of any type. Because many chat clients allow for the exchange of executable code, they present risks similar to those of email clients. As with email clients, care should be taken to limit the chat client's ability to execute downloaded files. As always, the user should be wary of exchanging files with unknown parties.

Now a day's virus and phishing attacks are also targeted through the Instant Messaging clients.

5.7 Securing Web Browser

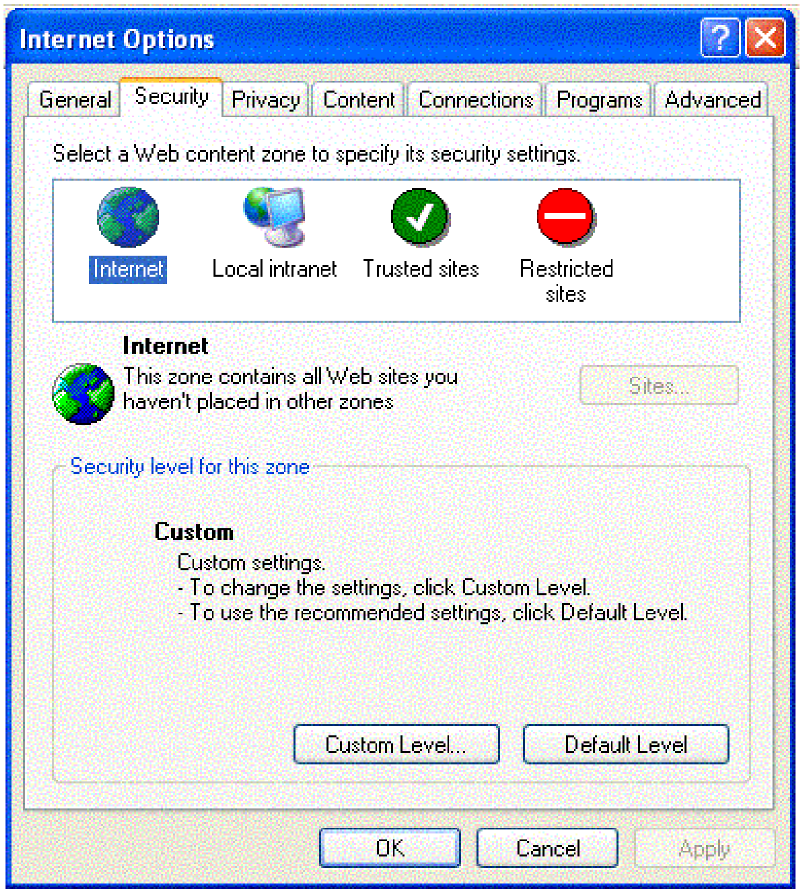
Web browsers are capable of parsing active code in many forms, including JavaScript, ActiveX, and Java code. These are automatically downloaded and executed by web browser. Malicious individuals often take advantage of this to attack systems, distribute malicious code, or negatively impact systems.

Microsoft Internet Explorer (IE) is installed as a default component of Windows Operating System and is closely integrated with it. Because of this, an exploitation of IE can seriously impact the underlying Windows installation, so it is critical to stay current with all IE updates. IE updates can be acquired through the **Windows Update** and Automatic updates features as described earlier.

5.7.1 Security Zones

IE uses a capabilities/trust model called **Zone Security**. In this model, Web sites are permitted to perform certain actions based on the following zones.

- **Restricted sites Zone**-This zone contains web sites that could potentially damage user's data.
- **Trusted sites zone**-This zone contains web sites that user can trust not to damage his computer or data.
- **Local Intranet Zone**-This zone contains all web sites that are on organization's intranet.
- **Internet Zone**- This zone contains all web sites that user haven't placed in other zones.



Select a Web content zone to specify its security settings.

Internet
This zone contains all Web sites you haven't placed in other zones

Security level for this zone

Custom
Custom settings.
- To change the settings, click Custom Level.
- To use the recommended settings, click Default Level.

Figure-3: Security zones in Internet Explorer

Each zone has an assigned security level (**High, Medium, Medium-Low, or Low**). Users can modify the security level for each zone, but IE will warn them if they attempt to assign a zone, a security level lower than the recommended minimum level.

5.7.2 Disable ActiveX and Java Scripts

Malicious web scripts can get to a web browser when a web developer sends such damaging code as part of the web server's response. This malicious code is then executed on the host running the browser.

Unfortunately the problem is by disabling these features; the user may find it frustrating that certain sites can no longer be effectively browsed. If the user cannot live without being able to run these scripts, then an alternative is to use a commercial anti-virus scanner that affords some level of protection against malicious scripts.

Choose the following options for safety:
Open Internet Explorer.

On the menu select **Tools → Internet Options**.

- Click on the **Security** tab.
- With the Internet zone highlighted, click the **Custom Level** button.
- Make the following modifications to the **Internet zone**:
- Under **ActiveX controls and plug-ins**, set **Script ActiveX controls marked safe for scripting** to **Disable**
- Under **Scripting,** set **Active scripting** to **Disable (**This will disable all scripting, including ActiveX. If this impacts required functionality, change the setting to **Prompt**)
- Under **Scripting,** set **Scripting of Java applets** to **Disable**

By default **Trusted sites zone** is assigned low security level, since this zone is intended for highly trusted sites, such as the sites of trusted business partners. User can also customize the settings by clicking on **Custom level** tab.

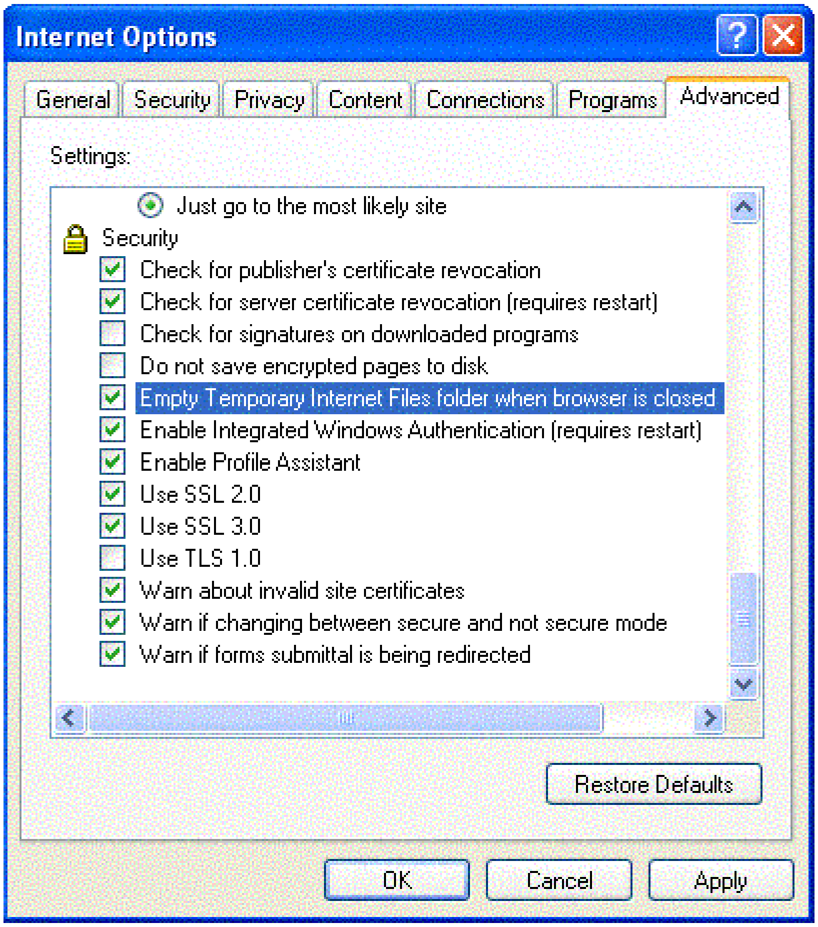
To add sites to this zone

- Click on **Trusted sites** icon
- Click on **sites** tab to add the trusted web site name
- Select **Require server verification (HTTPS:) for all sites in this zone -** This ensures that connections to the site are completely secure
- By default, the **Restricted sites zone** is assigned High security level. Assign sites to this zone as described earlier.
- Click on **OK** to return to the Internet Options box, and then click **OK**.

5.7.3 Other Security Settings in IE

IE contains many other security-related settings. Guidance on implementing a few of particular interest is as follows:

- Open Internet Explorer
- On the menu select **Tools → Internet Options**
- Click on the **Advanced** tab
- Under **Security**, check the box for **Check for server certificate revocation**. This causes IE to verify that a Web site’s digital certificate has not been revoked before accepting it as legitimate and current
- Under **Security**, check the box for **Empty Temporary Internet Files folder when browser is closed**. This causes IE to delete temporary files after the browser session is finished; these files could inadvertently contain sensitive information.



Settings:

● Just go to the most likely site

Security

☑ Check for publisher's certificate revocation
☑ Check for server certificate revocation (requires restart)
□ Check for signatures on downloaded programs
□ Do not save encrypted pages to disk
☑ Empty Temporary Internet Files folder when browser is closed
☑ Enable Integrated Windows Authentication (requires restart)
☑ Enable Profile Assistant
☑ Use SSL 2.0
☑ Use SSL 3.0
□ Use TLS 1.0
☑ Warn about invalid site certificates
☑ Warn if changing between secure and not secure mode
☑ Warn if forms submittal is being redirected

Figure-4: Other security settings for IE

- Click on the **Privacy** tab, and then click the **Advanced** button
- Check the **Override automatic cookie handling** box. This allows different settings to be made for handling first-party and third-party cookies
- Change the **Third-party Cookies** setting from **Accept** to **Prompt**. This setting causes IE to prompt the user to accept each third-party cookie that is presented to the system

For more information on Internet Explorer look at the home page of IE at

http://www.microsoft.com/windows/ie/default.mspx

5.7.4 Secure Site Identification

When buying online, the user must be sure doing business on secure Web sites. Unscrupulous "hackers" can exploit insecure sites to steal user's personal and important information such as credit card number. This information could be used to steal user's identity.

Most e-commerce Web sites secure user's personal information by encrypting or scrambling the data. Netscape and Internet Explorer users can check Web site security by following these instructions:

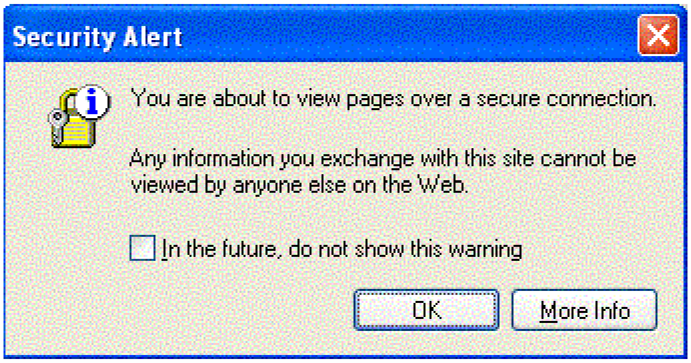
1. Look for the Lock symbol 🔒

Check the status bar at the bottom of the Web browser window for an unbroken lock symbol. This means user's personal information is scrambled, and no one can read it but the e-business he has contacted.

2. Look for "https" in the Web Site's Address

Secure sites will change their beginning from "http" to “https” if the information is about to pass through a secure channel. The "s" stands for "secure" and indicates that information will travel the Internet in encrypted form.

Since user's data is encrypted or scrambled, it can't be read during transmission. For example in www.hotmail.com when user enters the login and password information, the address bar indicates a change from “http” to “https” and also shows the following message before forwarding the information.



Security Alert

You are about to view pages over a secure connection.

Any information you exchange with this site cannot be viewed by anyone else on the Web.

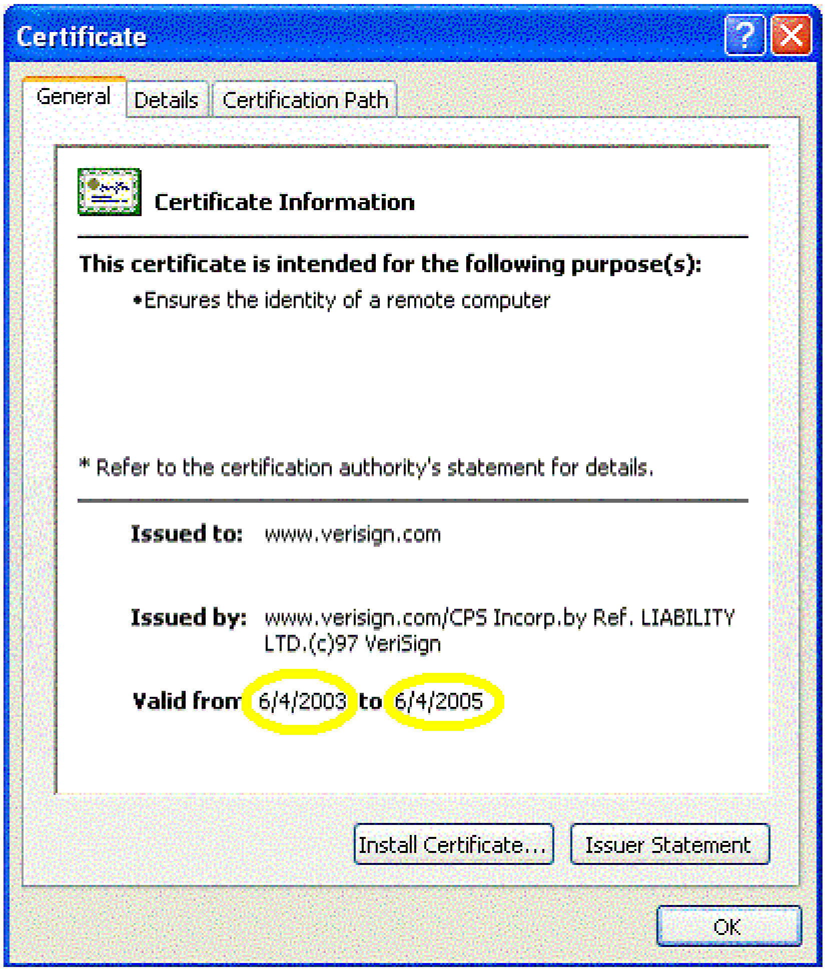
☐ In the future, do not show this warning

Figure -5: Message for secure connection

This warning message is generally ignored by the user or they just select it not to show in future, which is a bad practice. Whenever a security confirmation is made, user should verify the server's digital certificate.

5.7.5 Check the Certificate

Double-click on the lock symbol to view the security certificate. Make sure the certificate is "Issued to" the Web site and the "Valid from" dates are current. User can also see the certificate from **File → Properties** and then choose **certificates.**



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

* Refer to the certification authority's statement for details.

Issued to: www.verisign.com

Issued by: www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign

Valid from 6/4/2003 to 6/4/2005

Figure-6: Checking the validity of a certificate

The certificate should be checked for the issuer, to whom it has been issued and validity period of the issued certificate (as shown in the figure above).

6. Defensive Measures at Data Layer

This is the fourth and core layer of the defense in depth model. The defensive measures that have to be taken at this layer are:

- User must backup his important files
- Use encryption to ensure confidentiality of sensitive data
- File Checksum
- Password Policy
- Login Settings
- Audit Policy Settings
- Event Viewer

6.1 User must backup his Important Files

Taking backups of important files is one of the important safety measures to be taken. It's like keeping a spare tyre in the car while driving. Imagine the situation when one of the car's tyre punctures and when driver is about to change that, he come to know that he does not have a spare tyre with him? Or what happens if the computer system malfunctions or is destroyed by a successful attacker?

Backing up data is a task user should perform regardless of whether his system is secured or not. As far as security is concerned, this is the last line of defense. If someone gains access to the system and delete files, then user will need to restore them from backup.

Confused!!!- Which file to save and which not. Here is a help to discriminate between the two. Generally files are divided in two broad categories:

- Files which can be replaced: like basic operating system or application files.
- Files which can't be replaced: like family pictures, letters, invoices and account records etc.

Although it is the best practice to backup the whole system, but the constraint is of space available on the backup media. User can backup data to an external or removable hard drive, a personal tape drive, Zip or Jazz drive, CD-burner or a DVD-burner or bare minimum on to floppy. If user has a CD-writer (which may take more than one CD to take full backup) or DVD-writer he can conveniently take the full backup of his system. But if user does not have these two then he has to decide formerly about the files he wants to take backup and according to the space requirement he can select his backup media.

Every Operating System provides the feature to take backups on different media. Apart from that different applications are also available which can take the backups like the application which come with CD- writer or DVD-writer.

There is an in-built program that comes with Windows Operating System which is called as “Backup”. It is located at **Start>Programs> Accessories>System Tools,** and is quite easy to operate. User just has to select the files for backup and the destination where he want to store.

How and where should user store his backup media after he backup data to them? Well, user needs to store them in a safe place—remember that they contain files that are virtually irreplaceable if lost or damaged. If user does not have a secure storage area, it must not let this to prevent him from doing regular backups: any backup is better that no backup!

The definition of regularity depends on the comfort level of the user, i.e. how much work is one prepared to lose? A daily backup would be ideal but a weekly backup might be more viable.

6.2 Use encryption to ensure confidentiality of sensitive data

With the newer versions of Windows, i.e. Windows 2000 and XP, the user can use the Encrypting File System (EFS) to encrypt important data files. By using such encryption, an intruder who gets through the entire defense in depth layers and tries to access encrypted files or folders will be prevented from doing so. The intruder will receive an access denied message if he tries to open, copy, move, or rename an encrypted file or folder, unless the intruder has determined the UID and password of either the system administrator or the user who created the encrypted file.

Once a file or folder is encrypted, the user can work with the encrypted file or folder just as he would with any other file and folder since encryption is transparent to the user that encrypted the file. This means that the user does not have to decrypt the encrypted file before using it.

A file or a folder can be encrypted, subject to the following constraints, by using Explorer selecting the file/folder and clicking on the “Encrypt contents to secure data” attribute on the advanced features of the properties page:

- Can only encrypt files and folders on NTFS file system volumes.
- Compressed files or folders cannot be encrypted.
- System files cannot be encrypted.

If the user should ever lose their file encryption certificate and associated private key (through disk failure or any other reason), then data recovery is available through the person who is the designated recovery agent.

Of course if the use of EFS is not an option, then a knowledgeable user could use PGP for this sort of encryption. However, using PGP would not be transparent like using EFS. PGP Freeware is available for non-commercial use.

Apart form these; if the user is not using EFS or PGP, then he should use at least NTFS (NT File System), which gives file level user security. Windows 9x does not support NTFS file system, a user should have at least Windows NT or above to use NTFS.

6.3 File checksum

File Checksum is a utility that computes MD5 or SHA1 cryptographic hashes for files. The File Checksum utility can generate MD5 or SHA-1 hash values for files to compare the values against a known good value. It can compare hash values to make sure that the files have not been changed. It can also compute hashes of all critical files and save the values in an XML file database. It could be used to check the changes or compromise of the computer against the XML database to determine which files have been modified.

Users are advised to calculate checksum of all the system files and compare them regularly against the threat of Trojans or backdoors.

6.4 Password Policy

It’s a general practice of users to keep the same password for life long; rather users should change their passwords regularly.

Password should be complex and change regularly. Password policy setting controls the complexity of the password. To edit the password policy setting, go to **Start menu\Settings\Control Panel\Administrative Tools\Local Security Setting\Account Policy\Password Policy**\ set each and every option

- Enforce Password History
- Maximum Password Age
- Minimum Password Age
- Minimum Password Length
- Password Must Meet Complexity Requirement

Whenever the user is required to use a password, he should use a strong password that conforms to the following guidelines:

- At least seven characters in length (the longer the better)
- Includes upper and lower case letters, numerals, symbols
- Has at least one symbol character in the second through sixth position
- Has at least four different characters in given password (no repeats)
- Looks like a sequence of random letters and numbers
- Don’t use any part of logon name for the password

- Don’t use any actual word or name in ANY language
- Don’t use numbers in place of similar letters
- Don’t reuse any portion of old password
- Don’t use consecutive letters or numbers like "abcdefg" or "234567"
- Don’t use adjacent keys on the keyboard like "qwerty"

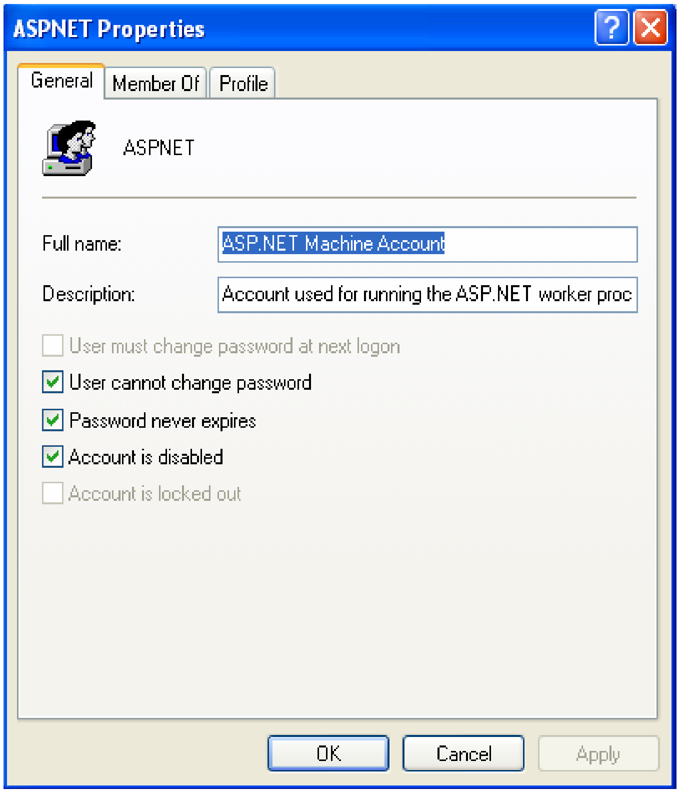
A good way to create a strong password is by using the first letters of a phase that user can easily remember.

6.5 Login settings

Windows NT, 2000 and XP come with many built in users and groups. These include the Administrator, Backup Operator, Guest, Power User and many more. The purpose of these groups is to enhance the abilities of a user without having to make that user an Administrator. However, due to the powers granted to these groups any user that is a member of one can become an Administrator. All unnecessary users must be disabled.

To disable unwanted accounts follow the steps as follows. Go to **Start menu\Settings\Control Panel\Administrative Tools\Computers Management\Local Users and Groups\Users**. Double click the account user want to disable and Check the box

Account is disabled



ASPNET

Full name: ASP.NET Machine Account

Description: Account used for running the ASP.NET worker proc

□ User must change password at next logon

☑ User cannot change password

☑ Password never expires

☑ Account is disabled

□ Account is locked out

6.6 Audit Policy Settings

User can set the Audit Policy Setting to determine the security events to report the user or system activity. For example, the user can choose to audit failed logon attempts, which might indicate that someone is trying to log on with an invalid password (perhaps using a program to automate the attack). Or user might want to monitor the use of a particular sensitive file. The user can also choose to monitor changes to user accounts and passwords, changes to security policies, and use of privileges that might reveal that someone is trying to "administer" user’s computer—perhaps not with user’s best interests in mind.

Unlike the other logs that appear in Event Viewer, the Security log is disabled by default in Windows XP Professional and Windows 2000. No events are written to the Security log until the user enable auditing, which is done via Local Security Settings. (In Windows XP Home Edition, security auditing is enabled for certain events. Because Home Edition doesn't include Local Security Settings, user cannot change which events are audited unless he use a tool like Auditpol.exe, which is included in the Windows 2000 Resource Kit.) Even if the user sets up auditing for files, folders, or printers, the events he specified aren't recorded unless he also enables auditing by setting a high-level audit policy in Local Security Settings.

To edit the Audit Policy Setting **Start menu\Settings\Control Panel\Administrative Tools\Local Security Settings\local Policies\Audit Policy** and check the boxes accordingly

The following table gives the Audit policy available in Windows Operating System with their respective descriptions.

Table-3: Audit Policies for Security Events

Policy	Description
Audit account logon events	Account logon events occur when a user attempts to log on or log off across the network, authenticating to a local user account.
Audit account management	Account management events occur when a user account or security group is created, changed, or deleted; when a user account is renamed, enabled, or disabled; or when a password is set or changed.
Audit directory service access	Directory service access events occur when a user attempts to access an Active Directory object. (If the computer is not part of a Windows domain, these events won't occur.)
Audit logon events	Logon events occur when a user attempts to log on or log off a workstation interactively.
Audit object access	Object access events occur when a user attempts to access a file, folder, printer, registry key, or other object that is set for auditing.
Audit policy change	Policy change events occur when a change is made to user rights assignment policies, audit policies, trust policies, or password policies.

Policy	Description
Audit privilege use	Privilege use events occur when a user exercises a user right (other than logon, logoff, and network access rights, which trigger other types of events).
Audit process tracking	Process tracking includes events such as program activation, handle duplication, indirect object access, and process exit. Although this policy generates a large number of events to wade through, it can provide useful information, such as which program a user used to access an object.
Audit system events	System events occur when a user restarts or shuts down the computer or when an event affects the system security or the Security log.

Local Security Settings has some additional policies that affect auditing, but they're not in the Audit Policy folder. Instead, look to the Security Settings\Local Policies\ Security Options folder for these policies:

- **Audit: Audit the user of Backup and Restore privilege.** Enable this policy if the user wants to know when someone uses a backup program to back up or restore files. To make this policy effective, user must also enable Audit Privilege Use in the Audit Policy folder.
- **Audit: Shut down system immediately if unable to log security audits.**
- **Audit: Audit the access of global system objects.** This policy affects auditing of obscure objects (mutexes and semaphores, for example) that aren't used in most home and small business networks; users can safely ignore it.

The user should only enable the audit policies which he requires to monitor. As it is a time-consuming process and can waste a lot of resources. When the auditing is enabled, the system must write an event record to the Security log for each audit check the system performs. This activity can degrade the computer’s performance. There is absolutely no need to enable them all, it’s purely on the requirement of the user, like Audit Directory Service Access is not required for the home user who is not connected to any Windows Active Directory network.

In addition, indiscriminate auditing adds to log many events that might be of little value to the user, thereby making the real security issues more difficult to find. And because the Security log has a fixed size, filling it with unimportant events could displace other, more significant events.

Here are some suggestions for what user should consider auditing:

- Audit failed logon attempts, which might indicate that someone is trying to log on with various invalid passwords.
- If the user is concerned about someone using a stolen password to log on, audit successful logon events.

- To detect use of sensitive files (such as a payroll data file, for example) by unauthorized users, audit successful read and write access as well as failed attempts to use the file by suspected users or groups.

- If the user use his computer as a Web server, he will want to know whether an attacker has defaced his Web pages. By auditing write access to the files that make up the Web pages, user will know whether his site has been vandalized.

- To detect virus activity, audit successful write access to program files (files with .exe, .com, and .dll file name extensions).

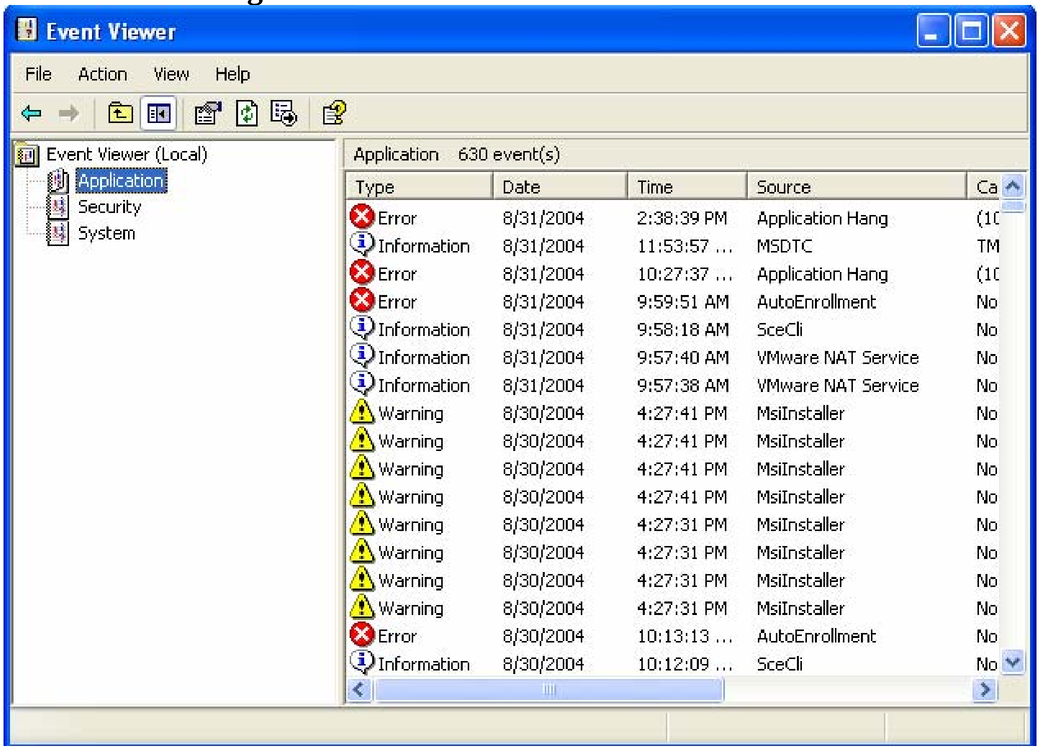
- If the user is concerned that someone is misusing administrative privileges, audit successful incidents of privilege use, account management, policy changes, and system events.

6.7 Event Viewer

A component a user can use to view and manage event logs, gather information about hardware and software problems, and monitor security events. It maintains logs of three kinds: application, system, and security.

Checkout for the security logs in event viewer regularly.

To open Event Viewer follow steps given below:
Start menu\Setting\Control Panel\Administrative Tools\ Event Viewer



Application 630 event(s)

Type	Date	Time	Source	Ca
Error	8/31/2004	2:38:39 PM	Application Hang	(1C
Information	8/31/2004	11:53:57 ...	MSDTC	TM
Error	8/31/2004	10:27:37 ...	Application Hang	(1C
Error	8/31/2004	9:59:51 AM	AutoEnrollment	No
Information	8/31/2004	9:58:18 AM	SceCli	No
Information	8/31/2004	9:57:40 AM	VMware NAT Service	No
Information	8/31/2004	9:57:38 AM	VMware NAT Service	No
Warning	8/30/2004	4:27:41 PM	MsiInstaller	No
Warning	8/30/2004	4:27:41 PM	MsiInstaller	No
Warning	8/30/2004	4:27:41 PM	MsiInstaller	No
Warning	8/30/2004	4:27:41 PM	MsiInstaller	No
Warning	8/30/2004	4:27:31 PM	MsiInstaller	No
Warning	8/30/2004	4:27:31 PM	MsiInstaller	No
Warning	8/30/2004	4:27:31 PM	MsiInstaller	No
Warning	8/30/2004	4:27:31 PM	MsiInstaller	No
Error	8/30/2004	10:13:13 ...	AutoEnrollment	No
Information	8/30/2004	10:12:09 ...	SceCli	No

7. References

http://www.microsoft.com
http://www.microsoft.com/technet/security
http://www.microsoft.com/technet/security/topics/desktopsecurity.mspx
http://www.securityfocus.com
http://www.cert.org
http://www.sans.org
http://csrc.nist.gov/itsec/
http://www.cert.org/homeusers/HomeComputerSecurity/
http://www.sans.org/rr/whitepapers/hsoffice/894.php
http://www.sans.org/rr/whitepapers/hsoffice/1033.php
http://www.sans.org/rr/whitepapers/hsoffice/625.php
http://www.sans.org/rr/whitepapers/hsoffice/624.php
http://www.sans.org/rr/whitepapers/hsoffice/622.php