Securing Your Windows Laptop

Arindam Mandal (arindam.mandal@paladion.net)
Paladion Networks (http://www.paladion.net) May 2004

Now-a-days laptops are part of our life. We carry laptops almost everywhere for our work, connect it to different networks and store our sensitive information on it. But we hardly care about the security of our laptop and that opens the door for an intruder to attack or steal sensitive data from it. An insecure laptop is susceptible to the following security risks:

- An attack to the laptop due to known vulnerabilities of Windows
- A Virus/Worm hit can paralyze your laptop
- Spywares installed on the laptop can steal your sensitive information
- An attacker can try network based attack to hack into your laptop
- Anybody can view/delete/modify your important files
- Malicious scripts embedded in the web pages can damage the laptop
- Easy to compromise the laptop due to insecure OS settings
- Attacker can use brute force/dictionary attack to break your weak password
- Insecure share in your laptop can be used to implant virus/worm/trojans
- An attacker can sniff your sensitive information from an insecure WLAN
- Laptop can be stolen

This paper describes how you can protect your Windows laptop easily.
Three easy ways to protect your laptop are:

- Secure your laptop OS -
    - Install OS with advanced security features and latest service packs.
    - Update the laptop with Windows Update.
    - Use only secure NTFS file system.
    - Protect your sensitive data with Encrypted File System (EFS).
    - Secure Internet Explorer's settings.
    - Disable non-essential services running on your laptop.
    - Tweak the security options for optimum security.
    - Configure strong password and account policy settings.
    - Secure the shares in your laptop.
- Reduce the surface of attack -
    - Install a personal firewall.
    - Install Antivirus and update it with latest virus definitions.
    - Install anti-spyware software to prevent spying.

- Other security measures -
    - Secure the Wireless LAN.
    - Physically secure your laptop.

Install OS with advanced security features and latest service packs

All Windows Operating Systems do not have the same level of security features. You should choose latest Windows OS which has security features built in. It is not recommended to use the following OS in your laptop:

- Windows 95
- Windows 98
- Windows Me

If you're installing a flavor of Windows, install only the following versions:

- Windows 2000 Professional
- Windows XP Professional

Use Windows XP Professional rather than Windows XP Home Edition. Windows XP Home Edition lacks many essential features (like EFS) which are present in Windows XP Professional. When you are buying a new laptop, remember to choose Windows XP Professional as your laptop OS.

Next step is to install the latest service pack for your laptop OS. A Windows service pack adds new features (including security features) to your OS and also installs latest security patches of Windows. Service pack protects your laptop from new vulnerabilities that were released till the release date of the service pack. Download the latest service pack for your Windows OS from: http://support.microsoft.com/default.aspx?scid=fh;en-us;sp

Backup all your essential data before installing a service pack. During the installation of service packs, always choose "Archive files" option so that you can uninstall the service pack later in case of any problems.

Update the laptop with Windows Update

Everyday, attackers are coming with new exploits in the form of Worm or Virus when a new vulnerability is found. The number of days between the reporting of a vulnerability and the release of an exploit are decreasing day by day.

For example, the RPC/DCOM vulnerability was reported to Microsoft on 1st July 2003. Microsoft released a patch (MS03-026) for this vulnerability on 16th July. A group called X-focus released an exploit code to the public on 25th July and the worm Blaster hit the world on 11th August 2003 exploiting this vulnerability. That's less than 6 weeks between the vulnerability being reported and the arrival of a worm.

It is important up-to-date your Windows OS with the latest security patches. It can be achieved by using Windows Update feature.

You can manually update your Windows OS easily if you have an internet connection. Type the following URL in your web browser and follow the instructions in the webpage to update Windows. http://windowsupdate.microsoft.com

If you don't have an internet connection, you can download the patches from the following website to another machine, copy those patches to your laptop and install them manually. http://www.microsoft.com/technet/security/current.aspx

You can also configure your Windows OS to download and install patches in the laptop automatically without your intervention. To keep your laptop updated using Windows Automatic Update please refer to the Appendix.

Use only secure NTFS file system

Windows NTFS file system provides file and folder level security. You can protect your important data using NTFS permission so that unauthorized users cannot access it. During the installation of Windows OS, format all the partitions of your laptop using NTFS. If you have existing FAT/FAT32 partition(s) on the laptop, you can convert it to NTFS without destroying your existing data using the `convert` command. To convert your FAT/FAT32 partition in NTFS, please refer to the Appendix.

Protect your sensitive data with EFS

EFS (Encrypted File System)[1] is a powerful security feature of NTFS file system in Windows 2000 and XP Professional that can be used for computers that plug in to a domain. Using this feature you can encrypt and secure your sensitive data. EFS can be implemented at file level and folder level. If you implement EFS at folder level, all files inside the folder will be encrypted using EFS. After encrypting a file or folder using EFS only you can open it with your login. Unauthorized users will not able to access your data. Even if your laptop is stolen; your sensitive data will be protected form disclosure. To protect your important data using EFS see the Appendix.

Secure Internet Explorer Settings

Some websites contains dangerous scripts and ActiveX controls. When you visit those websites, scripts are automatically downloaded and executed in your web browser.

[1] EFS is a good security feature of Windows 2000/XP. But if your laptop is not a part of a domain and its OS crashes, then it is not possible to recover encrypted data from laptop hard disk. Otherwise it is possible to recover using recovery agent account and certificate. So before using EFS decide if it meets your requirement, otherwise in the event of a disaster you might not able to recover your data. Please note that it is not recommended to encrypt your data using EFS in a standalone environment.

These malicious scripts can damage your laptop. Protect your laptop from this type of vulnerability by securing the Internet Explorer settings as mentioned below. For more details on how to configure the security settings of Internet Explorer please refer to the Appendix.

Section	Settings	Action
Scripting	Allow paste operations via script to prevent content from being exposed from your clipboard	Prompt
	Download signed ActiveX Controls	Prompt
	Download unsigned ActiveX Controls	Disable
	Initialize and script ActiveX Controls not marked as safe	Disable
Microsoft VM	Java permissions in order to properly sandbox the Java applet and prevent privileged access to your system	High safety
Miscellaneous	Access to data sources across domains to avoid Cross-site scripting attacks	Disable

Disable non-essential Services

Multiple services are enabled during default installation of Windows. Vulnerabilities in unused services can be used by malicious users to break in. Disable the non essential Windows services in your laptop to secure your laptop and also enhance the performance of your laptop. Following services are not needed for the proper operation of Windows on most laptops. For details on how to disable a service, please refer to the Appendix.

Non essential services
Alerter
Application Management
Clipbook
Distributed Link Tracking Client
Distributed Transaction Coordinator
Human Interface Device Access
IIS Admin (if IIS is not needed)
Indexing Service
Messenger
NetMeeting Remote Desktop Sharing
Network DDE
Network DDE DSDM
Network Provisioning Service
QoS RSVP
Remote Registry
Routing and Remote Access
Telnet
Windows Management Instrumentation Driver Extensions
WMI Performance Adapter

Tweak the Security Options for optimum security

A default installation of Windows has some insecure settings which may open the door to an attacker. These settings can be secured by configuring the security options of the

local computer policy. Please modify the settings in your Windows laptop as mentioned below. For details on how to modify the settings please refer to the Appendix.

Windows XP Professional Security Option Policy	Recommended Security Setting
Devices: Restrict CD-ROM access to locally logged-on user only	Disabled
Devices: Restrict floppy access to locally logged-on user only	Disabled
Interactive logon: Do not display last user name	Disabled
Interactive logon: Do not require CTRL+ALT+DEL	Disabled
Network access: Allow anonymous SID/Name translation	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Enabled
Network access: Do not allow storage of credentials or .NET Passports for network authentication	Enabled
Network access: Named Pipes that can be accessed anonymously	Delete All Entries
Network access: Remotely accessible registry paths	Delete All Entries

Windows 2000 Professional Security Option Policy	Recommended Security Setting
Additional restrictions for anonymous connections	No access without explicit anonymous connection
Do not display last user name in logon screen	Disabled
Restrict CD-ROM access to locally logged-on user only	Enabled
Restrict floppy access to locally logged-on user only	Enabled

Configure strong password and account policy settings

It is possible to get the password of your operating system account using brute force attack and dictionary attack. By default, the password policy setting in Windows is very weak. You need to protect your account by configuring strong password and account lockout policy, and of course using strong passwords accordingly. Configure the following settings in the account policy of your laptop. To learn how to modify these settings, please refer to the Appendix.

Password Policy	Recommended Security Setting
Enforce password history	5 passwords remembered
Maximum password age	30 days
Minimum password age	0 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store password using reversible encryption	Disabled

Account Policy	Recommended Security Setting
Account lockout duration	30 minutes
Account lockout threshold	5 invalid login attempts
Reset account lockout counter after	30 minutes

Secure shares in laptop

Windows sharing feature is very useful to share laptop resources (disk drive, printer, folders) in a network. But after sharing we usually forget to give secure permission on

the shared resources. Users are sometimes careless and forget to delete non-essential shares from our laptop. An intruder can get access to such insecure shares, download important files, delete or modify files and upload virus & Trojans in the laptop. The following steps guide you in protecting your shares:

- Only share the folders that are necessary to share.
- Restrict access to a share, so that only one user at a time can access it.
- Secure the permission on a share - remove everyone group and add only necessary user accounts to access the share.
- As far as possible give only 'read' access to your shares. Avoid granting write and full control access to the shares.
- Regularly check the existing shares in your laptop. Remove non-essential shares from it.

To learn how to secure the shares in your laptop, please refer to the Appendix.

Install a personal firewall to block attacks

A firewall reduces surface of attack of your laptop. With a personal firewall, you can minimize the attacks when you are connecting to different networks. Windows XP Professional comes with an inbuilt firewall. You can enable it for all your network connections. Older versions of Windows do not have the firewall feature. But many firewall software are available for download on the internet. Zone Alarm (http://www.zonelabs.com) is one such popular personal firewall. Download and install this software in your laptop and the firewall will protect your laptop from network based attack. To learn how to install the inbuilt firewall of Windows XP system, please refer to the Appendix.

Install Antivirus and update it with latest virus definitions

Worms and viruses are evolving daily. They are spreading so fast and in multiple variants that it is necessary to protect your laptop from infection. Internet is the main medium for viruses and worms to propagate. Viruses come from the internet via mail attachments, exploiting Windows vulnerabilities and infect your laptop. To safe-guard your laptop from virus/worm attack,

- Install Antivirus Software in your laptop. (some popular anti viruses in the market are – McAfee from Network Associates http://www.mcafee.com, Norton Antivirus from Symantec http://www.symantec.com and eTrust from Computer Associates http://www.ca.com)

- Update Antivirus Software's virus definition signature daily. You have several choices here - use automatic update feature of the anti virus software to update the signature or manually start the signature update program or download the latest virus definition from the internet and install it in your antivirus software.
- Always enable the automatic system protection feature of your antivirus software. This feature will protect you from any infection attempt to your laptop.
- Integrate the antivirus software with your e-mail client (e.g. Outlook or Outlook Express) so that all incoming and outgoing mails (including attachments) are scanned for virus.
- Scan you laptop once in a month with the Antivirus Software.

Install anti-spyware software to prevent spying

When you visit some web sites on the Internet, you could unknowingly be installing spyware software on your laptop. That spyware software can include trojans or activity tracking software or key logger[2] which is automatically installed in your machine. They can perform malicious activity in your laptop, silently monitor your activity and keystrokes and send it to the attacker. E.g. when you login to your bank's internet banking website using secret login ID and password, a spyware can track your visited web site's URL and get the secret login ID and password from your key strokes using key logger and send it to the attacker. To protect your laptop from spyware,

- Install Anti-Spyware software in your laptop. (Pest Patrol http://www.pestpatrol.com is a popular Anti-Spyware software in the market)
- Update spyware signature of the anti spyware software on daily basis.
- Always enable the automatic protection feature of your Anti-Spyware software. This feature will prevent any installation and malicious activity of spyware.
- Scan your laptop once in a month with the Anti-Spyware software to find any trace of spyware.

Wireless LAN Security

Wireless LANs (WLAN) have become popular today. We attach a WLAN card in the laptop and roam around with wireless network connectivity. WLAN is very popular in hotels, airport and other public places and generally used to access internet. Insecure settings in the WLAN configuration can be exploited by an attacker to sniff your sensitive information and steal your important data. You can identify an insecure WLAN by the following ways and should avoid participating in it.

[2] Modern Antivirus Software can detect Key logger software installed in the system.

- A WLAN that does not use WEP key for data encryption is very unsafe; anybody could break in and sniff your sensitive data. The most basic check of an insecure WLAN is to enable the wireless card and see if it connects to the WLAN without configuring a WEP key. It then means that WEP is not used and default secrets are used. So anybody else could also participate.
- If WEP is used in WLAN, it should be configured to use 128-bit keys with per-packet-keying. Else, it could be easily broken using WEP encryption cracking tools.
- Another basic check is to enable the wireless card and see if it automatically discovers a WLAN. It then means that SSID broadcast of the WLAN station is enabled. So anybody else could try to attack the network.

Do not connect to insecure WLAN. Before connecting to a WLAN always configure a strong WEP key of 128 bit length and secure your laptop as described before to increase the security and reduce the attack surface.

Physical Security

Laptop is a portable device and it can be easily stolen. Good physical security practices should be adopted to secure your laptop so that,

- Nobody can steal you laptop.
- Even if your laptop is stolen, nobody will be able to access your laptop.

To protect your laptop from theft, physically secure it with Laptop cable lock. It is a combination lock with a steel wire which can be attached to a laptop. Targus Notebook cable lock is a popular product. You can find more details about notebook cable lock at http://www.targus.com.

To protect you laptop from unauthorized access, set a system level complex BIOS password in your laptop. Thus when the laptop boots up it asks for the system password and unauthorized users will not be able to access your laptop.

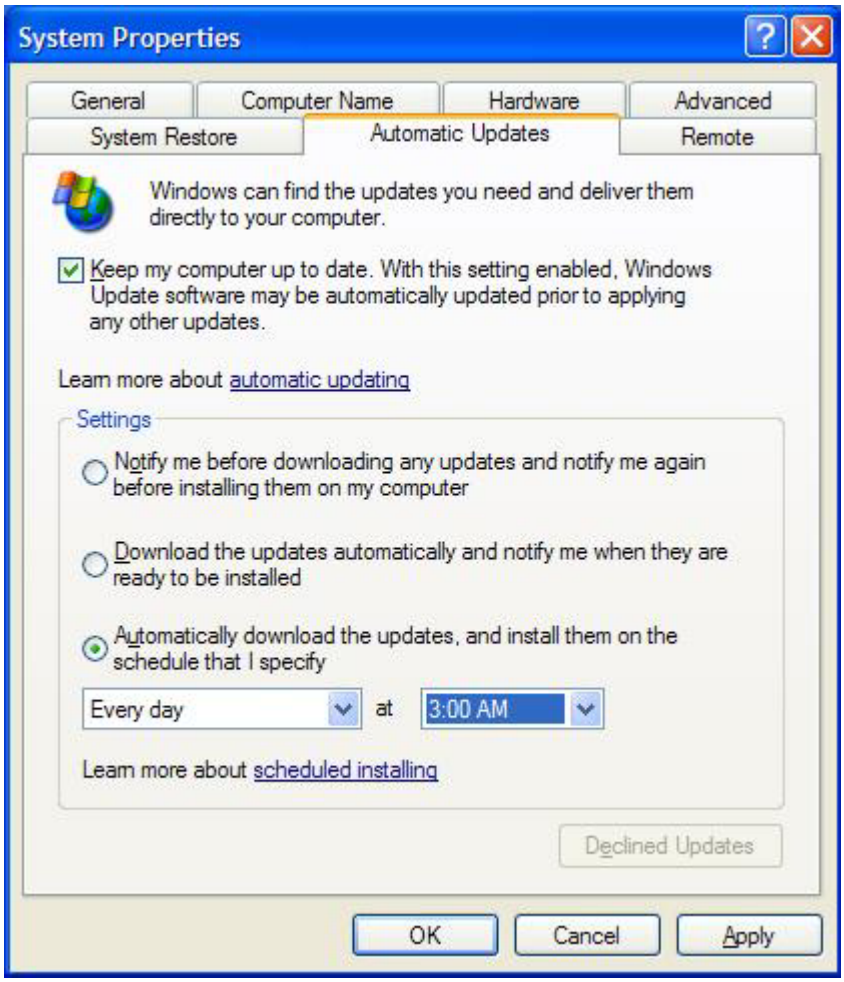
APPENDIX

Keep updated with Windows Automatic Update

Your laptop must be always connected to the internet to perform Automatic Update.

To keep updated your laptop using Windows Automatic Update:

1. Right click on **My Computer** icon on your desktop.
2. Select **Properties** from the menu.
3. Select **Automatic Updates** tab in System Properties page.
4. Check **Keep my computer up to date**.
5. Select **Automatically download the updates**, choose **Everyday** and a convenient **time**.
6. Click **OK**.



Convert FAT/FAT32 Partition to NTFS

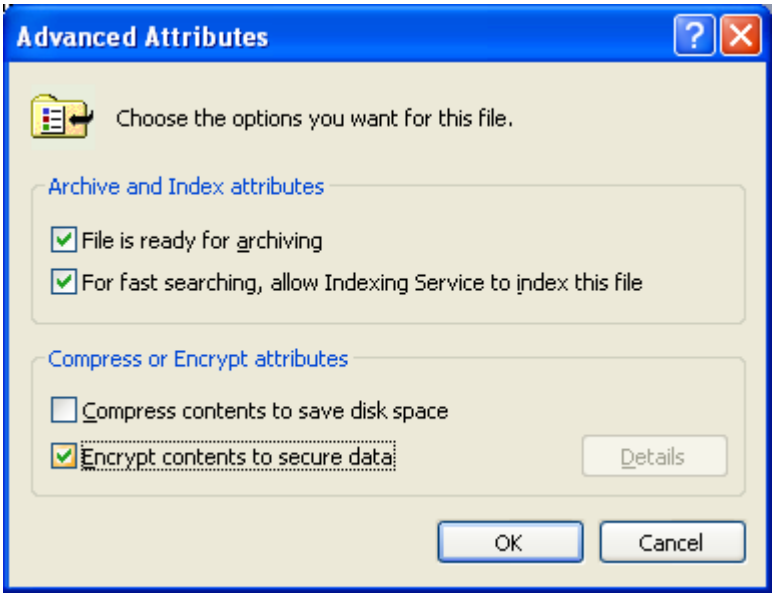
To convert FAT/FAT32 partition into NTFS:

1. Backup all data of the FAT/FAT32 partition.
2. Click **Start** > **Run**, type **cmd** and click **OK** to open the command prompt.
3. Type the following command:
   `convert x: /fs:ntfs (where x is the drive letter)`
4. Wait for completion of the conversion process.
5. Reboot the laptop.

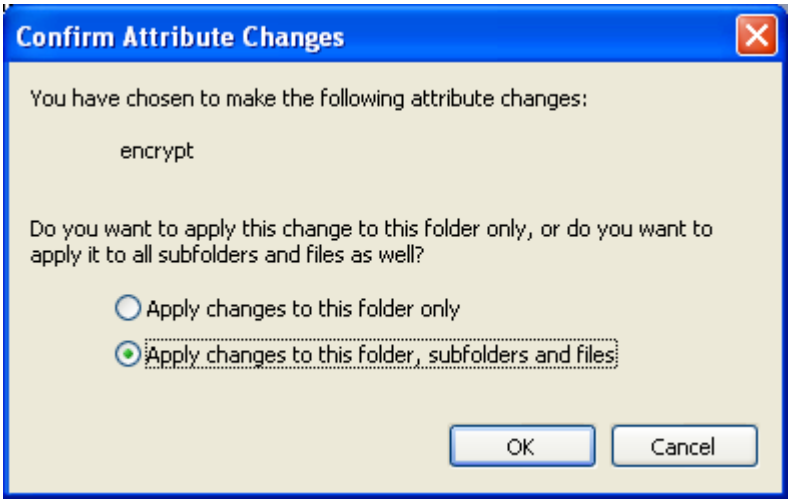
Protect your important data using EFS

To secure your sensitive data using Windows EFS (Encrypted file system):

6. Right click on the **File** or **Folder** in question.
7. Select **Properties** from the menu.
8. In the **General** tab of file or folder properties Click **Advanced** button.
9. In the Advanced attributes select **Encrypt contents to secure data**.



10. Click **OK**.
11. If you are encrypting a folder, then in **Confirm attribute changes** dialog select **Apply changes to this folder, sub folder and files** and click **OK**.



Internet Explorer Security Settings

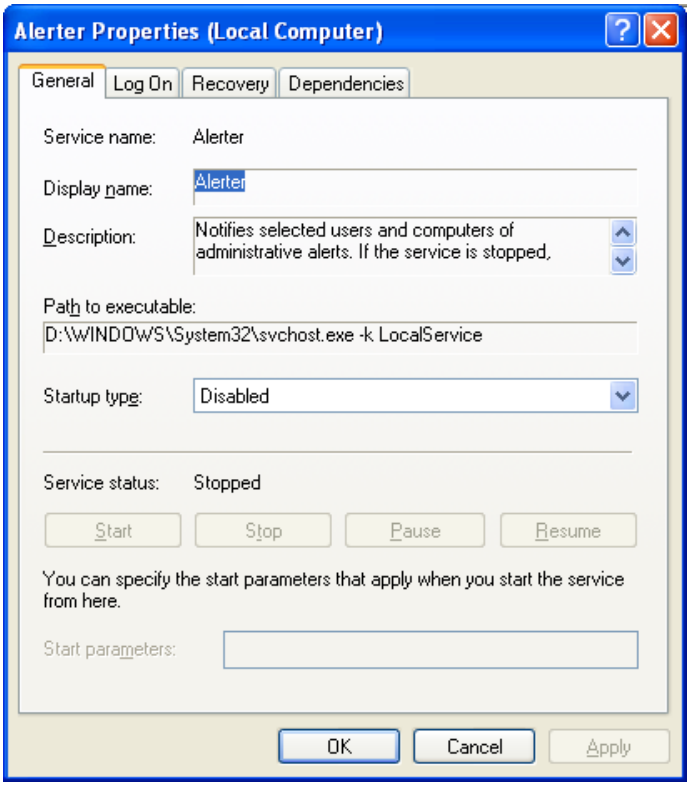
To secure Internet Explorer Settings:

1. Select **Internet Options** under the **Tools** menu in Inter Explorer browser.
2. Select the **Security** tab and then click **Custom Level** for the Internet zone.
3. Under **Scripting**, select **Prompt** for **Allow paste operations via script to prevent content from being exposed from your clipboard**.
4. Select **Prompt** for **Download signed ActiveX Controls**.
5. Select **Disable** for **Download unsigned ActiveX Controls**.
6. Also select **Disable** for **Initialize and script ActiveX Controls not marked as safe**.
7. Under **Microsoft VM**, select **High safety** for **Java permissions in order to properly sandbox the Java applet and prevent privileged access to your system**.
8. Under **Miscellaneous** select **Disable** for **Access to data sources across domains to avoid Cross-site scripting attacks**.

Disable a Service

To disable a service:

1. Click **Start** > **Run**, type **services.msc** and click **OK**.
2. In the service console select the service name in question and double click on it.
3. In the service properties page, under **General** tab, select the **Startup** type **Disabled** from drop down menu.
4. If the service is already running, stop the service by clicking on **Stop** button.
5. Click **OK**.



Modify Security Option

To modify the security option:

1. Click **Start** > **Run**, type **secpol.msc** and click **OK**.
2. In the local security settings console, go to **Security Settings** > **Local Policies** > **Security Options**.
3. In the right pane of the console, select the policy in question and double click on it.
4. In the properties of the policy, modify the settings as described in **Tweaking with Security Options**.

Modify Password and Account Policy

To modify the password and account policy:

5. Click **Start** > **Run**, type **secpol.msc** and click **OK**.
6. In the local security settings console, go to **Security Settings** > **Account Policy** > **Password Policy** or **Account Lockout Policy.**
7. In the right pane of the console, select the policy in question and double click on it.
8. In the properties of the policy, modify the settings as described in **Configure strong password and account policy settings**.

Secure Shares

To secure shares in your laptop:

1. Right click on the resource (Disk Drive or Folder) that you want to share.
2. Select **Sharing and Security** from the menu.

3. Select **Share this folder** and give a name of the share.
4. In **User limit** section, select **Allow this number of users** and set its value to **1**.
5. Click on **Permissions** button and remove **Everyone** group from access control list.
6. Add only the accounts of the users who actually need to access the share.
7. Select each and every user account, give only **Allow Read** permission and deselect other permissions.
8. Click **OK**.

To manage existing shares:

1. Click **Start** > **Run**, type **compmgmt.msc** and click **OK**.
2. Expand **Shared Folders** node and click on **Shares**.
3. In the right pane of the Computer Management console check the existing shares in your laptop. (Shares with $ at end, e.g. ADMIN$, are the default shares of the computer).
4. Find out the non essential shares in your laptop.
5. Right click on the non essential shares and select **Stop Sharing**.
6. In the confirmation dialog click **Yes**.
7. For other essential shares, right click on it and go to **properties**.
8. Go to **Share Permissions** tab and review the permissions on the share.
9. Modify the share permission as mentioned above in "secure shares in your laptop".

Configure Personal Firewall in Windows XP

To configure personal firewall in Windows XP professional:

1. Right click on **My Network Places** in the Desktop and select **Properties**.
2. Select the **Local Area Connection** or **Wireless Network Connection** icon, right click on it and select **Properties**.
3. In the **Properties** page, go to the **Advanced** tab and enable **Internet Connection Firewall**.
4. Now notice that a Pad Lock icon will come along with the Local area connection icon.