# UNIT 2 COMPUTER SECURITY

**Structure** **Page Nos.**



## 2.0 INTRODUCTION

In the previous unit we described threats to computer security, what are the reasons for these threats and various security techniques. In this unit we will provide you specific guidelines for establishing a secure Microsoft Windows 2000. This includes hardening operating system, File System, Local Security, various services, default accounts, network services etc.

## 2.1 OBJECTIVES

After going through this unit you will be able to secure:

- operating System;
- application Code;
- file System;
- local Security;
- services;
- default Accounts like guest and administrator, and
- network services etc.

## 2.1 HARDENING OPERATING SYSTEM AND APPLICATION CODE

The first step towards hardening is to make sure that your OS and Applications are up-to-date with service packs and hotfixes.

Microsoft periodically distributes large updates to its OS in the form of Service Packs. Service Packs include all the major and minor fixes up. Service Packs should be used in a test setup before being pushed into production due to the possibility of hidden or undetected bugs. If a test system is not available, wait a week or two after the release of a Service Pack, and monitor Microsoft Website for potential bug reports.

Microsoft also distributes intermediate updates to their operating systems in the form of Hotfix. These updates are usually small and address a single problem. Hotfixes can be released within hours of discovering a particular bug or vulnerability.

It is important to be aware that Service Pack and Hotfixes are not just applicable to Operating Systems. Individual applications have their own Service Pack and Hotfix requirements. The total security of the system requires attention to both operating system and application levels.

The process of discovering the appropriate Service Pack and hotfixes has been automated since the release of Windows 2000. The following steps describe the automated process of discovering and installing Service Packs and hotfixes to a Window 2000 system.

- Open IE (Internet Explorer)
- Go to Tools -→ Windows Update
- When asked if you trust Microsoft, say Yes.

Windows update will take some time to analyze your system. You will then be prompted with a listing of Service Packs or Hotfixes for your system. Additionally the following websites provide the necessary information for manual updates.

Security Bulletins: http://www.microsoft.com/technet/security/

Service Pack: http://www.microsoft.com/windows2000/downloads/servicepacks/

Hotfixes : http://www.microsoft.com/windows2000/downloads/critical/

Microsoft Windows Security: http://www.Microsoft.com/security

### ☞ Check Your Progress 1

1) Describe the strategy for hardening your windows 2000 operating system.

.....

.....

.....

.....

2) List the steps for discovering and installing services packs and hotfixes to a Windows 2000 system.

.....

.....

.....

.....

3) Fill in the blanks:

a) The first step towards hardening is to make sure that your OS and Applications are up-to-date with _____ and _____.

b) Service Packs should be used in a _____ before being pushed into production due to the possibility of hidden or undetected bugs.

c) The total security of the system requires attention to both _____ and _____.

## 2.3 HARDENING FILE SYSTEM SECURITY

The second step is to make sure that your hard drive partitions are formatted with NTFS (NT File System). This file system is more secure than FAT or FAT32 schemes.

**Step 1: Check your hard drive partitions**

- Log in as Administrator
- Double click on My Computer
- Right Click on each Hard Drive and Choose properties
- General Tab will identify the File System type.

**Step 2: Converting FAT or FAT32 partitions to NTFS**

- Go to Start →RUN
- Type cmd and click OK
- At command prompt issue the following command convert drive /FS:NTFS /V
- Hit return to run the command
- Reboot the system.

## 2.4 HARDENING LOCAL SECURITY POLICIES

The third step is to modify the default local security policy. While many system attacks take advantage of software inadequacy, many also make use of user accounts. To prevent such sort of vulnerability, "Policies" or rules define what sort of account/ password "behavior" is appropriate, what type of auditing is required. The configuration of user account policies is inadequate or disabled in a default installation.

Account policies answers the following:

- How often do I need to change my password?
- How long or how complex does my password need to be?

Auditing policies determine what kind of security transactions are recorded in the Security Event Log. By default, not is retained in the Security Event Log, so any attempt to compromise a system goes completely unrecorded. Logging events is critical for analysis in the aftermath of an intrusion incident.

The options given below can be set using the Local Security Policy editor on each individual computer. Nevertheless, Group Policy Configurations may override any changes made at the local level.

**Local Security Policy Editor Tool**

- Go to Start →Programs →Administrative Tools→ Local Security Policy
- Expand Account Policies by clicking the + box
- Select the appropriate category
- Double-click the individual policy setting to make the appropriate changes for the following.
- Password Policy
- Account Lockout Policy
- Audit Policy
- User Right Management
- Security Options
- When all settings have been configured, close the policy editor.

EVENT VIEWER

It is important to frequently check the Event Viewer to review log files for possible security concerns. You can access the Event Viewer by:

- Go to Start → Programs→ Administrative Tools -→ Event Viewer
- Go to Start →Programs →Administrative Tools→ Local Security Policy
- Expand Account Policies by clicking the + box
- Select the appropriate category
- Double-click the individual policy setting to make the appropriate changes for the following:
- Password Policy
- Account Lockout Policy
- Audit Policy
- User Right Management
- Security Options
- When all settings have been configured, close the policy editor.

## ☞ Check Your Progress 2

1) What steps will you take for hardening your Windows file system?

.....

.....

.....

.....

2) List the steps for converting a FAT files system to NTFS file system.

.....

.....

.....

.....

## 2.5 HARDENING SERVICES

The fourth step you take is to remove programs and services that are not required or needed. The more the number of applications that are installed on your system, the greater the risk of one of them containing a bug or security flaw.

The following is the list of services that can be disabled:

- Alerter: This service makes it possible for Windows 2000 computers to "alert" each other of problems. This feature is generally unused.
- Clipbook: The Clipbook Service is used to transfer clipboard information from one computer to another. This is generally used in Terminal Services.
- Fax Service: The Fax Service sends and receives faxes. It is generally unused.
- Messenger: The messenger service works in conjunction with alerter service and does .....
- NetMeeting Remote Desktop Sharing: Net Meeting users have the option to share their desktops, and allow other NetMeeting users to control their workstation.
- Telnet: The Telnet service allows a remote user to connect to a machine using command prompt.

## 2.6 HARDENING DEFAULT ACCOUNTS

The fifth step is to change the default configuration of the administrator and guest account. In general, a prospective user must have a login name and password to access a Windows 2000 system. The default installation creates an Administrator and Guest account. By changing these accounts name, system security is greatly enhanced.

Steps: Configuring Administrator Account

- Login as Administrator
- Go to Start→Programs→Administrative Tools→Computer management
- Open Local Users and Groups
- Click on the User Folder
- Right-click the Administrator Account, and choose to rename it. Make it a non-obvious name.
- Right click this renamed Administrator account and select "set password."

The Guest account is disabled in Windows 2000 by default. Enabling the guest account allows anonymous users to access the system. If you share a folder, the default permission is that Everyone has full control. Since the Guest account is included in "Everyone", system security is compromised. A standard practice is to always remove the share permissions from "Everyone" and add them to "Authenticated Users."

Steps: Configuring the Guest account

- Login as Administrator
- Go to Start→Programs→Administrative Tools→Computer management
- Open Local Users and Groups
- Click on the User Folder
- Right-click the Guest Account, and choose to rename it. Make it a non-obvious name.
- Right click this renamed Administrator account and select "set password."

## 2.7 HARDENING NETWORK ACTIVITY

Next step is to install a host based antivirus solution and firewall/intrusion detection system. This step will provide an added level and you can configure TCP/UDP ports that can be accessed. This step is to ensure that undesired communications are not occurring on ports.

### 2.7.1 Malicious Code

Type of Malicious Codes

- Viruses
- Worms
- Trojan Horses
- Back doors/Trap Doors
- Logic Bombs
- Bacteria/Rabbit

**A. Viruses**

A true virus is a sequence of code that is inserted into other executable code, so that when the regular program is run, the viral code is also executed. Viruses modify other programs on a computer, inserting copies of them.

**Different Types of Viruses**

**Boot Sector viruses**: They infect either the DOS boot sector or the master boot records of the disk and execute during booting.

**File infectors:** They attach themselves to executable files. These viruses are activated when the program is run.

**Macro viruses**: They come attached with documents with macro (built in program). When the document is opened the viruses are activated.

**Multipartite viruses**: They combine boot sector with file infector.

**Polymorphic viruses**: They alter themselves when they replicate so that anti-virus software looking for specific patterns known as signature, will not find them.

**B. Worm**

- Worms are programs that can execute independently and travel from machine to machine across network connections.
- They create a copy of themselves. This self-replication spreads worms like a flood in the networks causing slowdown and even breakdown of network communication services.

**C. Trojan Horses**

- It is a code that appears to be innocent and useful but it also contains a hidden and unintended function that presents a security risk. It does not replicate but it can steal passwords, delete data, format hard disks or cause other problems.

**D. Back Doors/Trap Doors**

- These are codes written into applications to grant special access to programs bypassing normal methods of authentication.
- This special code used by programmers during debugging can be present in released version, both unintentionally or intentionally, and is a security risk.

**E. Logic Bombs**

Logic bombs are programmed threats that lie dormant in commonly used software for an extended period of time until they are triggered when some pre-conditions are met like a particular day etc. Logic bombs come embedded with some programs.

**F. Bacteria/Rabbit**

These codes do not damage files. Their purpose is to deny access to the resources by consuming all processor capability/memory/disk space by self replicating.

**Damage caused by Malicious Codes**

The damage ranges from merely annoying to catastrophic ( loss of data services, disclosure of information).

Loss of reputation or legal consequences for software firm if s/he inadvertently ships software containing any malicious code.

**Who creates or writes virus code**

- Disgruntled employees
- Spies
- Experimenters
- Publicity Hounds
- Political activists

**Steps for protecting your system from viruses**

- Be careful about installing new software.
- Never install binaries obtained from untrustworthy sources.
- When installing new software, install it first on a non-critical system and test for bugs.

- Periodically review all system start-up and configuration files for changes.
- Turn off the automatic open on receipt feature from your email software.
- Before opening any attachments first scan it using updated anti-virus software.
- Regularly update anti-virus software engine and data files.
- Select "Hide File Extension" option.
- While opening any .doc file attachment using word disable macro.
- Turn off visual basic scripting.
- When not in use turn off the workstation or disconnect it from the network.
- Take regular backup of critical data and system files.

### 2.7.2 Firewell

A firewall is a safeguard one can use to control access between a trusted and a less trusted on. A firewall is a that:

- Enforces strong authentication for users who wish to establish connection inbound or outbound.
- Associates data streams that are allowed to pass through the firewall with previously authenticated users.
- A firewall is a collection of hardware, software and security policy.
- Without firewall, a site is more exposed to TCP/IP vulnerabilities, attacks from internet, and OS vulnerabilities.
- Due to increased number of hosts in a network, it is difficult to achieve host security through imposition of control on individual hosts.
- An intermediate system can be plugged between the private LAN (trusted network) and the public network (untrusted network).
- All traffic in and out of the trusted network can be enforced to pass through this intermediate system.
- This intermediate system is a good place to collect information about system and network use or misuse.
- This intermediate system is known as firewall.

**Why Firewall?**

- Protection from vulnerable services:
  - Filtering inherently insecure services like NFS/NIS.
  - Routing based attacks
- Controlled access to site system:
  - Prevent outside access except some special service like E-mail or HTTP
- Concentrated security:
  - All security measures like one time password and authentication software can be at the firewall as opposed to each host.

- Enhanced privacy:
  - Services like "finger" which displays information about user like last login, whether they have read e-mail etc., can be blocked.
  - IP addresses of the site can be shielded from outside world by blocking DNS service.
- Logging statistics on Network use or misuse:
  - All incoming and outgoing traffic from the Internet can be logged to provide statistics about the network usage. These statistics will provide the adequacy of control of firewall on network.
- Policy enforcement:
  - Provides means for implementing and enforcing a network control.

**Limitations of firewall**

- Restricted access to desirable services:
  - It may block services like TELNET, FTP, NFS, etc,. which user wants
  - Some network topologies require major restructuring from implementation of firewall.
- Large potential back door:
  - If modem access is permitted, attacker could effectively jump around the firewall.
- Little protection from insider attack:
  - Firewalls are generally designed to prevent outsider's attack.
  - Cannot prevent an insider from copying data, etc.
- Other Issues:
  - Firewall does not provide protection against users downloading virus-infected program from Internet or from E-mail attachments.
  - Potential bottleneck in throughput
  - Firewall, if compromised, will be a disaster.

**Primary Aspects**

The primary aspects of a firewall are:

- Firewall policy
- Packet filters
- Application Gateway
- Advanced authentication mechanism.

**Firewall Policy**

The firewall policy directly influences the design, installation and use of the firewall system.

**Higher Level Policy:** The Higher level policy addresses the services that will be allowed or explicitly denied from/to the restricted network.

- It is a subset of overall organisation's policy on security of its information assets.
- It focuses on Internet specific issues and outside network access ( dial-in policy, PPP connections, etc.).
- It should be drafted before the implementation of the firewall.
- It should maintain a reasonable balance between protecting the network from known risks while still providing Internet access to the users.
- Its implementation depends on the capabilities and limitations of the Firewall System.

Example

- No inbound access from Internet but allow outbound access from the network.
- Allow access from the Internet to selected systems like Web Server, Email Server, etc.
- Allow some users access from the Internet to selected servers but after strong authentication.

**Lower level Policy**: The Low level policy describes how the Firewall actually goes about restricting access and filtering the services that are defined in the Higher-level policy.

- The Lower level policy is specific to the Firewall and defines to implement the "Service Access Policy' already approved in Higher level Policy.
- Generally implements one of the two basic design policies:
  - Permit any service unless it is specifically denied
  - Deny any service unless it is explicitly permitted. This option is stronger and safer but difficult to implement.

**Packet Filter or Packet Filtering Gateways**

One type of firewall is the packet filtering firewall. In a packet filtering firewall, the firewall examines five characteristics of a packet

Source IP address
Source port
Destination IP address
Destination port
IP protocol (TCP or UDP)

Based upon rules configured into the firewall, the packet will be allowed through, rejected, or dropped. If the firewall rejects the packet, it sends a message back to the sender letting him know that the packet was rejected. If the packet was dropped, the firewall simply does not respond to the packet. The sender must wait for the communications to time out. Dropping packets instead of rejecting them greatly increases the time required to scan your network. Packet filtering firewalls operate on Layer 3 of the OSI model, the Network Layer. Routers are a very common form of packet filtering firewall.

A packet filter rule consists of two parts: An Action Field (BLOCK or DENY) and a Selection criteria (PERMIT or ALLOW).

Example: Sample Basic Packet Filters rule set.

| Sl. No. | Protocol | Source Address | Destination Address | Source Port | Destination Port | Action | Description |
|---|---|---|---|---|---|---|---|
| 1 | TCP | Any | 192.168.200.3 | >1023 | 80 | Permit | Allow inbound HTTP access to the host having IP address 192.168.200.3 |
| 2 | TCP | Any | 192.168.200.4 | >1023 | 21 | Permit | Allow inbound FTP control channel to the host having IP address 192.168.200.4 |
| 3 | TCP | Any | 192.168.200.4 | Any | 20 | Permit | Allow FTP data channel to this host |
| 4 | UDP | Any | Any | 53 | >1023 | Permit | Permit all inbound DNS resolution |
| 5 | Any | Any | Any | Any | Any | Deny | Cleanup rule blocking all traffic not included above. |

**Problems with Packet Filters**

- Packet filtering rules are complex to specify and difficult to test thoroughly.
- Exception to packet filtering rules sometimes can be unmanageable.
- Some packet filtering routers do not filter on the TCP/UDP source port, which can make the filtering rule set more complex and can open up "holes" in the filtering scheme.
- Problem of IP Fragmentation: If fragmentation of IP packet occurs only the first fragment keeps the TCP/UDP header information of the original packet, which is necessary to make filtering decision. Some packet filters may apply rules on the first fragmented piece, which is not serious for inbound traffic. For outbound traffic, even if the first fragmented piece is dropped other may go out leaving a serious security threat.

**Stateful Packet Filtering**

An improved form of the packet filtering firewall is a packet filtering firewall with a stateful inspection engine. With this enhancement, the firewall 'remembers' conversations between systems. It is then necessary to fully examine only the first packet of a conversation.

A stateful inspection peeks into the payload of data of the IP packets and takes out the required information on which the filtering can be done. A stateful inspection maintains the state information about the past IP packets.

- For robust security, a firewall must track and control the flow of communication passing through it.
- For TCP/IP based services, firewall must obtain information from all communication layers.

- State information, derived from past communications and other applications, are an essential factor in making the decision.

State information:

- Communication information from all layers in the packet.
- Communication derived from previous communications ( Example: The outgoing "Port" command of an FTP session could be saved so that an incoming FTP data connection can be verified against it).
- Application derived state from other application. ( Example: A previously authenticated user would be allowed access through the firewall for authorized services only).

**Application Proxy Firewall**

Another type of firewall is the application-proxy firewall. In a proxying firewall, every packet is stopped at the firewall. The packet is then examined and compared to the rules configured into the firewall. If the packet passes the examinations, it is re-created and sent out. Because each packet is destroyed and re-created, there is a potential that an application-proxy firewall can prevent unknown attacks based upon weaknesses in the TCP/IP protocol suite that would not be prevented by a packet filtering firewall. The drawback is that a separate application-proxy must be written for each application type being proxied. You need an HTTP proxy for web traffic, an FTP proxy for file transfers, a Gopher proxy for Gopher traffic, etc... Application-proxy firewalls operate on Layer 7 of the OSI model, the Application Layer.

**Application Gateway Firewall**

Application-gateway firewalls also operate on Layer 7 of the OSI model. Application-gateway firewalls exist for only a few network applications. A typical application-gateway firewall is a system where you must telnet to one system in order to telnet again to a system outside of the network.

- Gateway interconnects one network to another for a specific application.
- Gateway used in firewall configuration is an Application Level Gateway or a Proxy Server.
- The function of application Gateway is application specific. If an application Gateway contains proxies for FTP and TELNET, then only those traffics will be allowed and other services are completely blocked.
- Imposition of an application gateway breaks the conventional client/server model as each communication requires two connections one from the client and the other from the firewall to the server.

The Internet community often uses the term Bastion Host to refer to an exposed firewall system that hosts an application gateway.

Advantages of Application gateways:

- Information Hiding: The application gateway is the only host whose name is made known to the outside systems.
- Robust authentication and logging: All traffic can be pre-authenticated and logged to monitor the effectiveness of security policy.
- Less complex filtering rule: The packet filtering router needs only to allow traffic destined for the application gateway and reject the rest.

## 2.8 FAULT TOLERANT SYSTEM

A Fault tolerant system is designed by using redundant hardware (hard disk, disk controller, server as a whole) to protect the system in the event of hardware failure. There are various techniques to do that:

SFT ( System Fault Tolerance) Techniques

- Disk Mirroring: Data is writer in two separate disks, which are effectively mirror images of the each other. The disk mirroring technique is depicted in *Figure 1*.

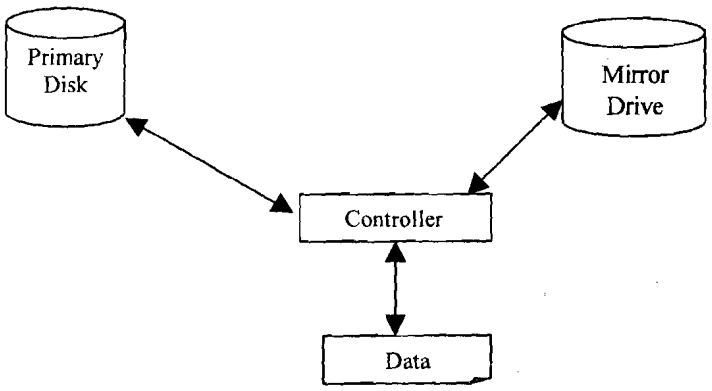


**Figure 1: Disk Mirroring**

- Disk Duplexing: Disk duplexing, shown in *Figure 2*, implements separate controller for each disk.

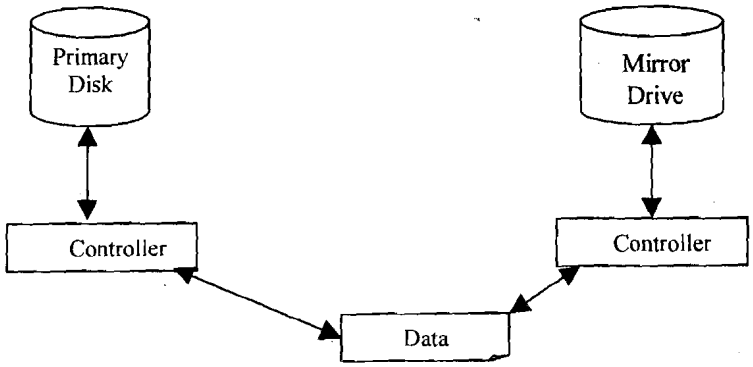


**Figure 2: Disk Duplexing**

- **RAID**

  The term RAID (Redundant Array of Independent Disks) was first coined by a research group at University of California, Berkeley, to describe a collection of disk drives (disk array), which can:

- Collectively act as a single storage system
- Tolerate the failure of a drive without losing data.
- Function independently of each other.

The RAID advisory board defines RAID levels and the most common levels are numbered from 0 to 6, shown in *Figure 3*, where each level corresponds to a specific type of fault tolerance.

| RAID Level | Fault Tolerance |
|---|---|
| Level 0 | Striping without parity |
| Level 1 | Mirroring / duplexing |
| Level 2 | Striping with ECC (Error Correction Code) |
| Level 3 | Striping with a dedicated parity disk |
| Level 4 | Independent data disks with shared parity disk |
| Level 5 | Independent data disks with distributed parity blocks (striping with parity) |
| Level 6 | Second parity |

**Figure 3: RAID Levels**

### Striping Without Parity

Disk striping is a technique where data is divided into 64K blocks and spread in a fixed order among all the disks in the array. Because it provides no redundancy, this method cannot be said to be a true RAID implementation. If any partition in the set fails, all data is lost. It is used to improve performance by spreading disk I/O over multiple drives.

This strategy requires between 2 and 32 hard disks. It provides the best performance when used with multiple disk controllers. The technique is shown below in *Figure 4*.

### Mirroring / Duplexing

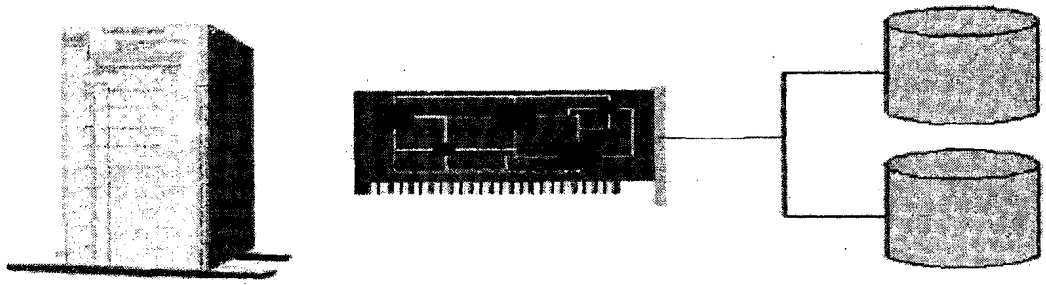

**Figure 4: Drive Mirroring**

**Mirroring** requires two hard disks and a single disk controller. It takes place at the partition level and any partition, including the boot/system partitions, can be mirrored. This strategy is the simplest way of protecting a single disk against failure.

In terms of cost per megabyte, disk mirroring is more expensive than other forms of fault tolerance because disk-space utilisation is only 50 percent. However, for peer-to-peer and modest server based LANs, disk mirroring usually has a lower entry cost because it requires only two disks. Stripe sets with parity (RAID level 5) require three or more.

Data is written simultaneously to both partitions/disks.

**Duplexing** is simply a mirrored pair with an additional disk controller on the second drive. This reduces channel traffic and potentially improves performance. Duplexing is intended to protect against controller failures as well as media failures.

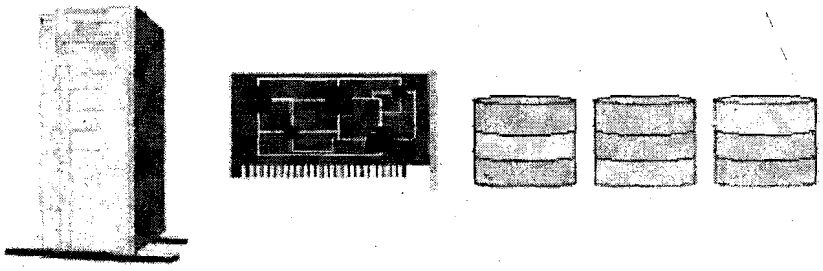

**Figure 5: Striping with Party (or RAID 5)**

Striping with parity (RAID 5) depicted in *Figure 5*, is the most common strategy for new fault tolerance designs. It differs from other levels in that it writes the parity information across all the disks in the array. The data and parity information are managed so that the two are always on different disks. If a single drive fails, enough information is spread across the remaining disks to allow the data to be completely reconstructed.

Stripe sets with parity offer the best performance for read operations. However, when a disk has failed, the read performance is degraded by the need to recover the data using the parity information. Also, all normal write operations require three times as much memory due to the parity calculation.

Striping with parity requires a minimum of three drives and up to thirty-two drives are supported. All partitions except the boot/system partition can be part of a stripe set.

The parity stripe block is used to reconstruct data for a failed physical disk. A parity stripe block exists for each stripe (row) across the disk. RAID 4 stores the parity stripe block on one physical disk, while RAID 5 distributes parity evenly across each of the disks in the stripe set.

**Implementing RAID**
It is possible to implement RAID using either hardware or software.

**Hardware Solutions**
Some vendors implement RAID level 5 data protection directly into hardware, as with disk array controller cards. Because these methods do not require software drivers, they generally offer performance improvements. In addition, some hardware implementations allow you to replace a failed drive without shutting down the system. The disadvantages of a hardware implementation are that they can be very expensive and may lock you into a single vendor solution.

SCSI controllers can be purchased with dual interfaces and built-in logic to implement a hardware-level RAID system. This can be used with any operating system, even if the operating system itself is not RAID-aware.

**Software Solutions**
Both Windows NT Server and NetWare provide the option to set up software fault tolerance using standard disks and controllers.

**Mirroring Versus Stripe Sets with Parity**
Implementing a fault tolerance strategy will require some trade-off depending on the level of protection required. The major differences between disk mirroring and striping with parity are **performance** and **cost**.

Overall, **disk mirroring** offers better I/O performance and has the advantage of being able to mirror the boot/system partition. Because mirroring utilises only 50% of available disk space, it tends to be more expensive in cost per megabyte. As hard-disk prices decrease, these costs will become less significant.

**Disk striping with parity** offers better read performance than mirroring, especially with multiple controllers. This is because the data is split among multiple drives. However, the need to calculate parity information requires more system memory and can slow down performance considerably. The cost per megabyte is much lower with striping because the disk utilisation is much greater.

### Clustering

It is a collection of computers, which work together like a single system. If a computer in the cluster crashes other surviving computers can serve the client request.

A combination of clustering and disk mirroring can be used to provide a very secure system, in addition to maintaining integrity and high availability it gives scalability.

## 2.9 BACKUP AND UPS

Why backup?

The backup is required to recover valuable data and to restore system in the event of disaster due to:

- User/ System-staff error
- Hardware / Software failure
- Crackers/Malicious code
- Theft
- Natural Disaster
- Archival of information

### Types of Backup

- Complete or Full backup
    - Every file on the source disk is copied.
    - It clears the archive bits of the all the files of the source disk.
    - Slowest but most comprehensive.
    - Restoring from full backup is straightforward.
- Incremental backup
    - Copies only those files for which the archive bit is set.
    - Clears the archive bit after backup.
    - Saves backup time and backup media.
    - Restoration has to be done first from the full backup tapes from the incremental backup tapes in order of creation.

- Differential Backup
  - It is only the backup of the files, modified since the last full or incremental backup.
  - It does not alter the archive bit setting.
  - Takes more space than incremental backup.
  - Restoration is simple, restore from the full backup and the latest differential backup.

CASE STUDY: Windows 2000 Backup Strategies

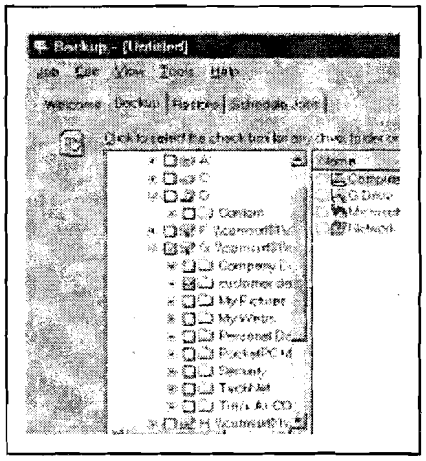

**Figure 6: Windows 2000 Backup**

One of the most important operations in a network system is the creation of a secure backup. Typically, backups take place using a tape system that has the advantage of high capacity, relatively low cost and portability. When you click on backup option, screen as displayed in *Figure 6* will be presented to the user.

**Backup Methods**

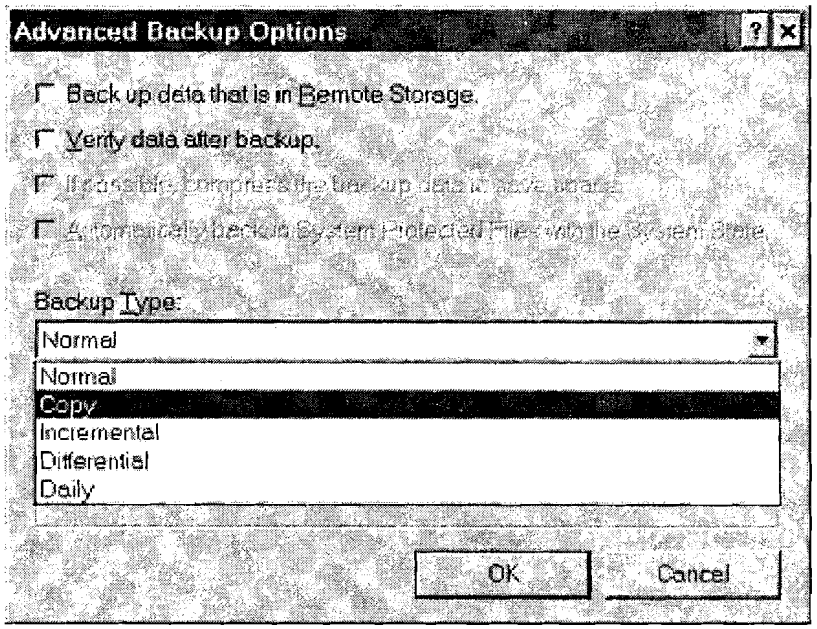


**Figure 7: Choosing the Backup Type**

A backup may be performed using one of three methods as shown in *Figure 7*:

- Full
- Incremental
- Differential

A full backup includes all selected files and directories while incremental and differential backups check the status of the archive attribute before including a file. The archive attribute is set whenever a file is modified. This allows backup software to determine which files have been changed, and therefore need to be copied.

The criteria for determining which method to use is based on the time it takes to restore versus the time it takes to back up.

Assuming a backup is performed every working day, an incremental backup only includes files changed during that day, while a differential backup includes all files changed since the last full backup.

Incremental backups save backup time but can be more time-consuming when the system must be restored. The system must be restored from the last full backup set and then from each incremental backup that has subsequently occurred. A differential backup system only involves two tape sets when restore is required.

*Table 1* summarises the three different backup types:

**Table 1: Three different backup types**

| Type of backup | Data that will be backed up | Time for backup / restore | State of archive attribute |
|---|---|---|---|
| **Full** | All selected data regardless of when it has previously been backed up | High/low (one tape set) | Cleared |
| **Incremental** | New files and files modified since the last backup | Low/high (multiple tape sets) | Cleared |
| **Differential** | All data modified since the last full backup | Moderate/ moderate (no more than 2 tape sets) | Not Cleared |

Doing a full everyday backup on a large network takes a long time. A typical strategy for a complex network would be a full weekly backup followed by an incremental or differential backup at the end of each day.

- The advantage of using a **full daily backup** is that only one tape set is required to restore the system.
- The advantage of an **incremental backup** is that it takes less time to back up but several tape sets may need to be restored before the system is operational.
- The advantage of a **differential backup** is the balance of time for both restoring and backing up.

Example: Power Management in Windows 2000 as shown in *Figure 8.*

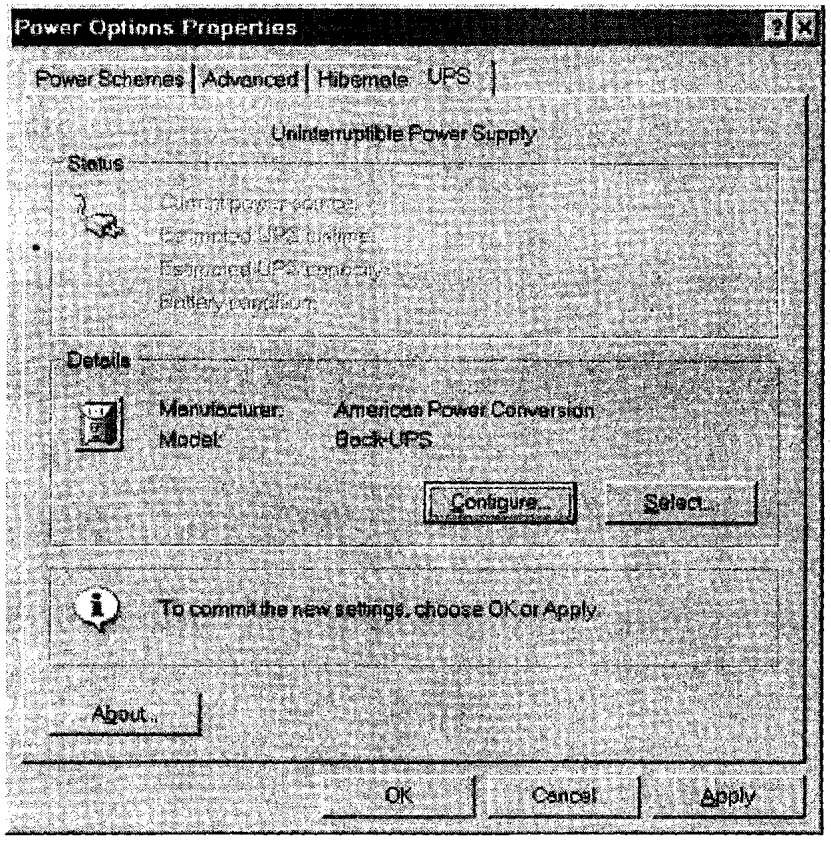


**Figure 8: Selecting your UPS in Windows**

## UPS (Uninterruptible Power Supplies)

**UPS** (Uninterruptible Power Supplies) **provide an alternative AC power supply in the event of power failure and also eliminate the effects of** power surges **and** spikes.

Generally a UPS comprises the following:

- A bank of batteries and associated charging circuit.
- A DC-to-AC converter to generate AC voltage from batteries.
- A switch over circuit to allow the UPS to take over from the (failed) supply.
- Spike and surge protection circuitry.

Most UPS fall into one of the following categories:

### Offline UPS

An offline UPS keeps the batteries charged all the time but does not operate the inverter until the power fails and the inverter starts and is switched into the power circuit.

Offline UPS are cheaper to build and do not dissipate as much heat as the online varieties but they have one drawback - switchover time.

It takes a small amount of time for an offline UPS to detect a power failure, start the inverter and switch it into the power circuit. This delay can be just a few milliseconds and is not usually 'noticed' by the equipment to which it is connected. However, this is not always the case and some equipment will not work properly with an offline UPS.

### Online UPS

An online UPS is constantly supplying power from the batteries and inverter, while at the same time, charging the batteries from the incoming supply. The benefit of this design is that there is no switchover delay when the power fails.

### Choosing a UPS

Choosing the right type of UPS is relatively straightforward. The following guidelines assist the choice but should be used in conjunction with the information available from the equipment and UPS manufacturers.

### Offline or online

Check the type of UPS that is suitable for the equipment to be protected.

### Power rating

The maximum power rating (and hence cost) of a UPS is determined by the battery specification and the power handling of the inverter and other circuitry. Each UPS is rated according to the maximum VA (power) they can supply without overloading.

To find out the required VA rating of a UPS

= Sum ( Watt Used by Each Device ) * 1.6

### Operational time

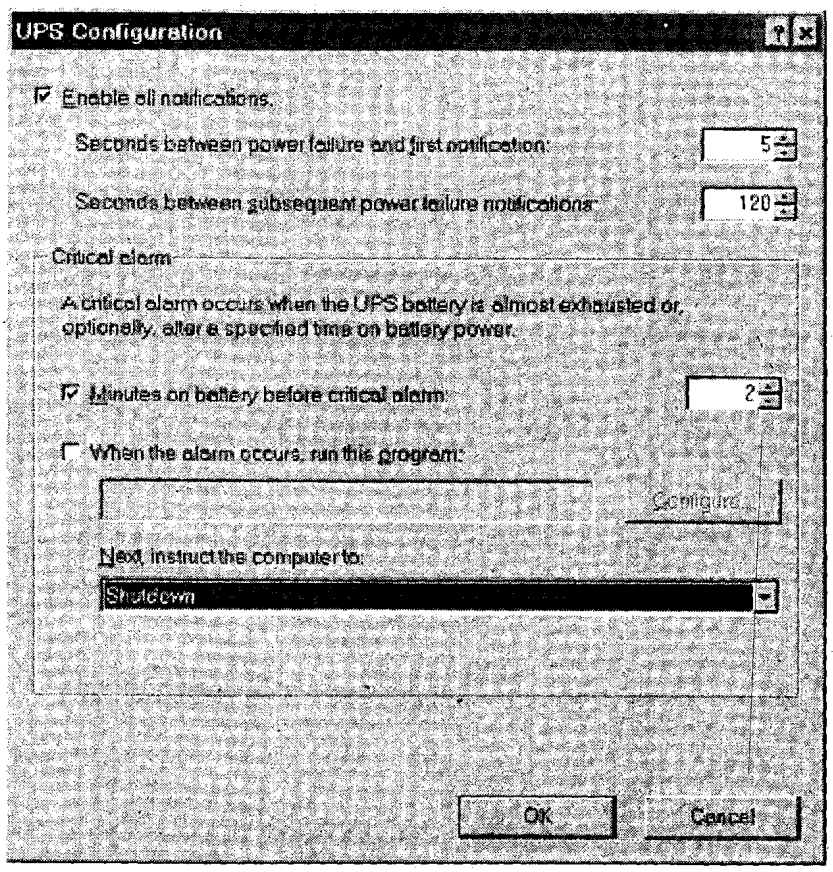


Figure 9: Configuring the UPS

The number of batteries within the UPS determines the amount of time for which it can generate and supply power (the 'up time'). Most vital computer systems require UPS power for at least five minutes. This gives the time needed for correct shut down in the event of a general power failure. The various options for configuring your UPS are shown in *Figure 9*.

Additional Considerations when Choosing a UPS.

- **UPS monitoring**

Some UPS's can be connected to their host system via a serial port or an add on card; the UPS can then alert the host system when there is a power failure or an impending problem such as 'battery power low'.

**Network monitoring**

Some UPS can communicate with monitoring software such as SNMP (the Simple Network Management Protocol) via a network connection.

## ☞ Check Your Progress 3

1) List the steps for hardening default accounts (Guest and Administrator accounts).

.....

.....

.....

2) List different types of malicious code.

.....

.....

.....

3) List advantages and limitations of firewall.

.....

.....

.....

4) Expand the following:

   a) RAID

   b) UPS

5) Describe backup strategies for your system.

.....

.....

.....

6) How will you select a UPS for your system.

.....

.....

.....

7) Discuss and compare existing virus protection tools.

.....

.....

.....

## 2.10 SUMMARY

With proper setting and hardening Operating System, Application Code, File System, Services, Network Service, Default Accounts, Virus Protection, and Proper backup strategies, we can secure our Windows 2000 System from known vulnerabilities and attacks. However, to counter new attacks and vulnerabilities, it is desired that the latest security measures should be implemented under expert guidance.

## 2.11 SOLUTIONS/ANSWERS

### Check Your Progress 1

1) The strategy for hardening Windows 2000 security are: (a) hardening operating system and applications, (b) hardening file system, (c) hardening local security policies, (d) hardening services, (e) hardening default accounts, (f) hardening network services, (g) dealing with malicious codes, (g) installing firewall, fault tolerant system, backup and UPS.

2) Steps are:

- Open IE ( Internet Explorer)
- Go to Tools -→ Windows Update
- When asked if you trust Microsoft, say Yes.

3) a) Service Packs and Hotfixes

b) Test setup

c) Operating System and Application.

### Check Your Progress 2

1) a) Check your hard drive partitions and (2) convert FAT or FAT32 partitions into NTFS partitions.

2) Converting FAT or FAT32 to NTFS partitions:

- Go to Start →RUN
- Type cmd and click OK
- At command prompt issue the following command convert drive FS:NTFS/V
- Hit return to run the command
- Reboot the system

## Check Your Progress 3

1) Steps: Configuring Administrator Account:

- Login as Administrator
- Go to Start→Programs→Administrative Tools→Computer management
- Open Local Users and Groups
- Click on the User Folder
- Right-click the Administrator Account, and choose to rename it. Make it a non-obvious name
- Right click this renamed Admiinistrator account and select "set password"

Steps: Configuring the Guest account

- Login as Administrator
- Go to Start→Programs→Administrative Tools→Computer management
- Open Local Users and Groups
- Click on the User Folder
- Right-click the Guest Account, and choose to rename it. Make it a non-obvious name.
- Right click this renamed Admiinistrator account and select "set password"

2) **Malicious codes**

- Viruses
- Worms
- Trojan Horses
- Back doors/Trap Doors
- Logic Bombs
- Bacteria/Rabbit

3) **Firewall**

**Advantages**

- Protection from vulnerable services
- Controlled access to system
- Concentrated security
- Enhanced privacy
- Logging statistics on network use and misuse
- Policy enforcement.

**Limitations**

- Restricted access to desirable services
- Large potential backdoors
- Little protection from insider attack.

4) a) RAID - Redundant Array of Independent Disks

b) UPS - Uninterruptible Power Supplies

5) Backup Strategies are:

— Complete Backup

— Incremental Backup

— Differential Backup

6) Selecting a UPS

The following criterias are considered :

a) **Offline or Online:** Check the type of UPS that is suitable for the equipment to be protected.

b) Power rating: To find out the required VA rating of a UPS apply the following formula.

= Sum [Watt (power) used by each device] *1.6 each device

c) UPS Monitoring

d) Networking Monitoring

7) Discuss and Compare Nortan, Officescan and other Virus tool. Take informention from their respective websites.

## 2.12 FURTHER READINGS

1) Security Bulletins: http://www.microsoft.com/technet/security/

2) Service Pack: http://www.microssoft.com/windows2000/downloads/servicepacks/

3) Hotfixes : http://www.microsoft.com/windows2000/downloads/critical/

4) Microsoft Windows Security: http://www.Microsoft.com/security