UNIT 1 SECURITY CONCEPTS

Structure **Page Nos.**

1.0 INTRODUCTION

Computer Security can be defined as technological and managerial procedures applied to computer systems to ensure the availability, integrity, and confidentiality of the information managed by the computer. It means the protection of Integrity, Availability and Confidentiality of Computer Assets and Services from associated Threats and vulnerabilities.

Security is divided into two categories; (a) computer security and (b) network security. In generic terms, computer security is the process of securing a single, standalone computer; while network security is the process of securing an entire network of computers.

a) **Computer Security:** Technology and managerial procedures applied to computer systems to ensure the availability, integrity, and confidentiality of the data managed by the computer.

(b) **Network Security:** Protection of networks and their services from unauthorised modification, destruction, or disclosure and provision of assurance that the network performs its critical functions correctly and there are no harmful side effects.

The major weakneses in a computer system pertain to hardware, software, and data. However, other components of the computer systems may also be targeted.

1.1 OBJECTIVES

After going through this unit you will be able to:

- know of the threats to computer security;
- understand what causes these threats, and
- know various security techniques.

1.2 GOALS OF COMPUTER SECURITY

The goals of computer security are integrity, confidentiality, and availability of the information managed by the computer system. The relationship among the three is shown in *Figure 1*.

1.2.1 Integrity

The data Integrity in computer security deals with the knowledge that data has not been modified. Data Integrity is related to data accuracy, but integrity and accuracy are not the same. For example, if information is entered incorrectly, it will remain incorrect. So, it is possible to have Data Integrity without Data Accuracy.

Integrity means preventing unauthorised modification. To preserve the integrity of an item means that the item is unmodified, precise, accurate, modified in an acceptable way by authorised people, or consistent.

1.2.2 Confidentiality

Confidentiality means preventing unauthorised access. It ensures that only the authorised person accesses the computer system. Not all data available on the computer falls in the category of confidential data. There is data that can be made public and there is data that is considered sensitive. It is this critical or sensitive data that will require confidentiality. Data confidentiality cannot be enforced unless data integrity is present. The following items could require data confidentiality: credit card files, medical records, personnel data, mission-critical data, and R&D data etc.

1.2.3 Availability

There is no point in making the computer system so secure that no users can access the data they need to perform their jobs effectively.

The system should be accessible to authorised persons at appropriate times.

A computer system is available if:

- The response time is acceptable
- There is a fair allocation of resources
- Fault tolerance exists
- It is user friendly
- Concurrency control and deadlock management exists. Terms like concurrency

control and deadlock management will be discussed in the operating system course.

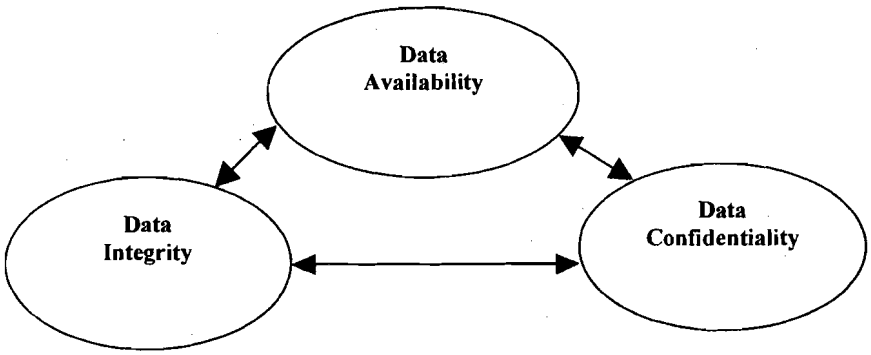


Figure 1: Relationship between Confidentiality, Integrity, and Availability

1.3 SECURITY PROBLEM AND REQUIREMENTS

Protection of information has been a major challenge since the beginning of the computer age. The computer security problem has grown with the computer industry, the computer itself was not really part of the security problem or its solution.

Connecting computers introduces a need for communication security (often utilising cryptography) to prevent the possibility of an attack. Connecting computers gives them greater accessibility, which increases computer security problems.

Computer security attempts to ensure the confidentiality, integrity, and availability of the computing system's components. The principal components of a computing system subject to attacks are: hardware, software and data. These three components and the communications among them is the basis of computer vulnerabilities. Attackers can devise attacks that exploit these vulnerabilities. There are basically four kinds of attacks on computing systems: **interception**, **interruption**, **modification**, and **fabrication**. These terms will be explained later.

One of the ways to identify security problems is by means of risk analysis. Risk analysis involves determining:

- What you need to protect,
- What you need to protect it from,
- And how to protect it.

It is the process of examining all of your risks, and ranking those risks by level of severity.

There are three major steps in risk analysis, namely:

- Identifying the assets (what are you protecting)
- Identifying the threats (against what)
- Identifying impact.

1.3.1 Identifying the Assets

List all the things that are subject to security threats. These include:

- **Hardware:** CPUs, boards, keyboards, terminals, workstations, personal

computers, printers, disk drives, communication lines, terminal servers, routers, hubs, gateways, servers, modems, etc.

- **Software:** source programs, object programs, utilities, diagnostic programs, operating systems, communications program, firewall software, IDS (Intrusion Detection System) software etc.
- **Data:** during execution, store on-line, archive off-line, backup, audit logs, databases, in transit over communication media etc.
- **People:** user, people needed to run systems.
- **Documentation:** on programs, hardware, systems, local administrative procedures.
- **Supplies:** paper, forms, ribbons, floppy diskettes, magnetic media.

Based on the above, asset inventory can be created with the following component for each asset:

- Designated owner
- General support system or critical/major application
- Physical/logical location.

1.3.2 Identifying the Threats

Once the assets requiring protection are identified, it is necessary to identify threats to those assets. The threats can be then evaluated to determine what potential for loss exists.

There are two basic type of threats: accidental threats and intentional threats.

Accidental threats can lead to exposure of confidential information or causing an illegal system state to occur due to modification of information. An intentional threat is an action performed by an entity with the intention to violate security. And this includes destruction, modification, fabrication, interruption or interception of data.

In general, threats to an asset should be considered in terms of the availability, confidentiality and integrity of the asset. The possible threats to a computer system can be:

- Unauthorised Access
- Disclosure of information
- Denial of service.

1.3.3 Identifying the Impact

After identifying the assets and threats, the impact of security attack should be assessed. The process includes the following tasks.

- Identifying the vulnerabilities of the system;
- Analysing the possibility of threats to exploit these vulnerabilities;
- Assessing the consequences of each threat;
- Estimating the cost of each attack;
- Estimating the cost of potential counter measure, and
- Selecting the optimum and cost effective security system.

The consequence of a threat materialised in an organisation could result in one or more impacts. For example, an impact can be:

- Infringement of privacy
- Financial loss
- Disruption of activities.

1.4 THREATS AND VULNERABILITIES

With the rise of multiprogramming, the several aspects of a computing system requiring protection are system software, memory, sharable I/O devices such as disk, printers, tape drivers, shared programs/procedures, networks, shared data, files, and execution environment.A threat is a set of instances that has the capability of causing loss or harm to the computer system. There are many threats to a computer system and can be (a) Human initiated, (b) Computer initiated, and (c) Natural disasters like flood or earthquake.

A threat can be accidental or deliberate and the various types of security breaches can be classified as (a) interruption, (b) interception, (c) modification and (d) fabrication.

- Interruption: An asset of the system becomes lost, unavailable, or unusable.
    - Malicious destruction of a hardware device
    - Deletion of program or data file
    - Malfunctioning of an Operating system.
- Interception: Some unauthorised entity can gain access to a computer asset. This unauthorised entity can be a person, a program, or a computer system.
    - Illicit copying of program or data files
    - Wiretapping to obtain data.
- Modification: Some unauthorised party not only accesses but also tampers with the computer asset.
    - Change in the values in the database
    - Alter a program
    - Modify data being transmitted electronically
    - Modification in hardware.
- Fabrication: Some unauthorised party creates a fabrication of counterfeit object of a system. The intruder may put spurious transaction in the computer system or modify the existing database.

An attacker needs three things (1) method, (2) opportunity and (c) motive.

- A method: It comprises the tools, skills, knowledge etc.
- Opportunity: Opportunity means the right time and right access to perform the attack.
- Motive: Motive is the reason to carry out the attack.

A **threat** can be blocked by control of vulnerability. We can use a control as a protective measure. A control can be in action, device, procedure and technique that limits or eliminates vulnerability.

A computer system has three valuable components as pointed out earlier: hardware, software and data. Vulnerability is a weakness in the system. This weakness may be exploited by threats causing loss/damage or harm to the system. Vulnerability does not cause any harm until exploited. It can be a weakness in: (a) Procedures, (b) Design and (c) Implementation.

The various vulnerability examples are: insufficient security training, lack of security awareness, inadequate recruitment procedures, insufficient preventive maintenance, lack of identification and authentication mechanisms, transfer of password in readable form (clear text), unprotected public network connections, poor password management, well-known flaws in the software, unsupervised work by external staff, no security policy, exposed/unprotected communication lines, poor cable joint, inadequate system management, no audit-trail, wrong allocation of access rights or permissions, lack of documentation and dialup connections, etc.

The computing system vulnerabilities are:

- Software vulnerabilities: software vulnerability can be due to interruption, interception, modification, or fabrication. The examples of software vulnerabilities are: (a) destroyed/deleted software, (b) stolen or pirated software, (c) unexpected behaviour and flaws, (d) non-malicious program errors, (e) altered (but still run) software.
- Hardware vulnerabilities: hardware vulnerability is caused due to interruption (denial of service), modification, fabrication (substitution) and interception (theft).
- Data vulnerabilities: Data vulnerability is caused by interruption (results in loss of data), interception of data, modification of data and fabrication of data.
- Human vulnerabilities: The various human generated vulnerabilities are break-ins, virus generation, security violation, inadequate training.

☞ Check Your Progress 1

1) What are the Goals of Computer Security?

.....

.....

.....

2) Justify the following statement:

" There is no confidentiality without integrity"

.....

.....

.....

.....

1.5 USER AUTHENTICATION

Authentication in a computer system uses any of three qualities to authenticate the user:

- Something the user knows, like password, PIN numbers; pass phrases, a secret handshake etc.
- Something the user has: Identity badges, physical keys, a driver's license, or a uniform.
- Something the user is: This is based on the physical characteristic of the user (Biometrics), such as a finger print, face recognition, voice recognition etc.

Two or more methods can be combined for more solid authentication; for example, an identity card and PIN combination.

The computer system needs a system in place to be sure that only authorised users have access to its resources. On the computer system, one of the critical areas of security is who has access to what.

There are two types of access control that can be implemented:

- Mandatory Access Control (MAC) : MAC is an access control policy that supports a system with highly secret or sensitive information. Government agencies typically use a MAC.
- Discretionary Access Control (DAC) : DAC is an access control policy that uses the identity of the user or group that they belong to allow authorised access. It is discretionary in that the administrator can control who has access, to what and what type of access will they have, such as create or write, read, update, or delete.

Authentication occurs when a user provides the requested information to an authentication verification authority. The traditional method of authentication is to provide a password.

To increase the level of reliability, biometric authentication can be introduced. The user is not only identified digitally, but by their physical characteristics such as fingerprint scan, iris scans or hand geometry.

Authentication Token: It is a portable device used for authenticating a user. The tokens are devices that operate by using systems such as:

Hardware Tokens

- **Challenge and response:** It is an authentication technique using a calculator type of token that contains identical security keys or algorithms as Access Server, which sends an unpredictable challenge to the user, who computes a response using their authentication response token.
- **Time-based challenge response Token:** The Time-based Token utilises an authentication method where the security token and server use an identical algorithm. To gain access, the user takes the code generated by the token and adds his or her user name and PIN to create a pass code. The pass code is combined with a seed value and the current time, encrypted with an algorithm and sent to the server. The server authenticates the user by generating its own version of the valid code by accessing the pre-registered PIN and using the same seed value and algorithm for validation.

Software Token

If an organisation does not wish to purchase hardware tokens, it may opt for a software type instead. A software token is an authentication process using portable devices such as a Palm Pilot, Palm PC, or wireless telephone to carry the embedded software.

1.6 SECURITY SYSTEM AND FACILITIES

Security controls should be installed and maintained on each computer system or computer node to prevent unauthorised users from gaining entry to the information system and to prevent unauthorised access to data.

System software and resources should be accessible after being authenticated by access control system.

1.6.1 System Access Control

- Access to information system resources like memory, storage devices etc., sensitive utilities and data resources and programme files shall be controlled and restricted on "need-to-use" basis.
- The access control software or operating system should be providing features to restrict access to the system and data resources. The use of common passwords such as "administrator" or "president" or "game", etc,. to protect access to the system and data resources should be avoided.
- Guidelines and procedures governing access authorisation shall be developed, documented and implemented.
- Each user shall be assigned a unique user ID.
- Stored passwords shall be encrypted using internationally proven encryption techniques to prevent unauthorised access.
- Automatic time-out for terminal inactivity should be implemented.
- Audit trail of security sensitive access and actions shall be logged.
- Audit trails must be protected against modification or deletion.
- Activities of all remote users shall be logged and monitored closely.
- The startup and shutdown procedure of the security software must be automated.
- Sensitive operating system files must be protected using proven tools and techniques.

1.6.2 Password Management

Certain minimum quality standards for password shall be enforced. The following control features shall be implemented for passwords:

- Minimum of 8 characters without leading or trailing blanks;
- Shall be different from existing passwords;
- To be changed at least once every 90 days and for sensitive systems it should be changed every 30 days;
- Should not be shared, displayed or printed;
- Password retries should be limited to a maximum of 3 attempted logons after which the user ID shall then be revoked for sensitive systems;

- Passwords, which are easy to guess, should be avoided;
- Password shall always be of encrypted form to avoid disclosure, and
- All passwords must be resistant to dictionary attacks and all known password cracking algorithms.

1.6.3 Privileged User Management

The following points must be taken into account while granting privilege to users.

- Privileges shall be granted only on a need-to-use basis.
- Login available only from console.
- Audit log should be maintained.

1.6.4 User Account Management

Procedures for user account management should be established to control access to application and data. It should include:

- Should be an authorised user.
- A written statement of access rights should be given to all users.
- A formal record of all registered users shall be maintained.
- Access rights of users who have been transferred, or left the organisation, shall be removed immediately.
- A periodic check/review shall be carried out for redundant user accounts and access right that is no longer required.
- Redundant user accounts should not be reissued to another user.

1.6.5 Data and Resource Protection

All information shall be assigned an owner responsible for integrity of data and resource. This will help in protection of data and resources to a great extent. And this assignment of responsibility should be formal and top management must supervise the whole process of allocation of responsibilities.

1.6.6 Sensitive System Protection

- Security token/smart cards/bio-metric technologies such as iris recognition, finger print verification technologies, etc,. shall be used to complement the usage of password to access the computer system.
- Encryption should be used to protect the integrity and confidentiality of sensitive data. In this unit we will discuss various techniques used in the protection of sensitive computer systems and networks.

Data backup and Off-site Retention

- Backup procedures shall be documented, scheduled and monitored.
- Upto date backup of critical items shall be maintained. These items include: data files, utilities/programmes, databases, operating system code, encryption keys, documentation, full/incremental backup frequencies as per schedule.

Firewall

The firewall is the first line of defense for any computer system or network. All packets that enter the network should come through this point. A modern firewall is a system of applications and hardware working together. A sophisticated firewall

performs a combination of packet filtering, network address translation (NAT), and proxy services. These applications are depicted in *Figures 2, 3* and *4* respectively.

Firewalls have two general methods of implementing security for a network. Although variations between these two exist, most modifications belongs to one or the other of the following:

— packet filtering and

— proxy server (Application Gateway)

Packet Filtering were designed to look at header information of the packet. Packet Filtering, shown in *Figure 2*, was the first type of firewall used by many organisations to protect their network. The general method of implementing a packet filter was to use a router. These routers had the ability to either permit or deny packets based on simple rules.

Proxy Servers use software to intercept network traffic that is destined for a given application. The proxy server, shown in *Figure 3*, recognises the request, and on behalf of the client makes the request to the server. In this, the internal client never makes a direct connection to the external server. Instead, the proxy functions as man-in-the-middle and speaks to both the client and server, relaying the message back and forth. The addition of proxy server capabilities added to the firewalls created a much more solid security product than a pure packet filter. Proxy software can make decisions based on more than the header information of a packet.

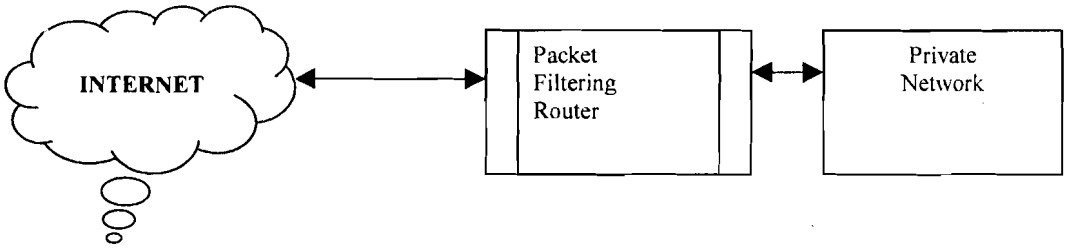


Figure 2: Packet Filtering Router

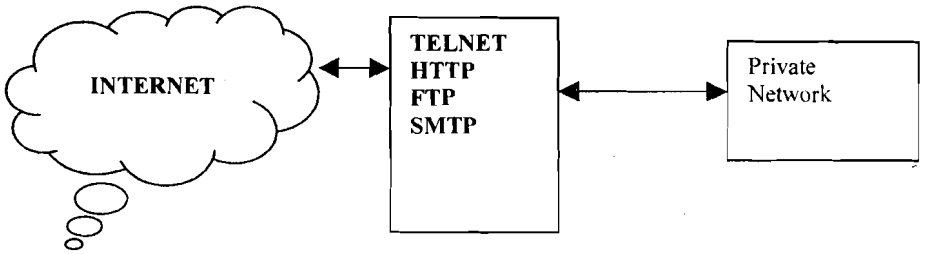


Figure 3: Application level gateway or Proxy server

A firewall can have a negative impact on the network by blocking access to the desired resources. This is due to improper configuration of a firewall that makes the desired resource unavailable. Additionally, if an ordinary PC has been configured to be the firewall (a multi-homed computer) it may not have the internal speed to perform all the functions of the firewall fast enough, resulting in increased latency.

Encryption

- Central to all security mechanism
- Confidentiality of data

- Some protocols rely on encryption to ensure availability of resources.

The encryption process as a whole is taking data that is plain text (readable form), and using a mathematical technique to make the text unreadable. The receiver then performs a similar technique to decrypt the message. The process of encrypton and decrypton is shown in *Figure 4*.

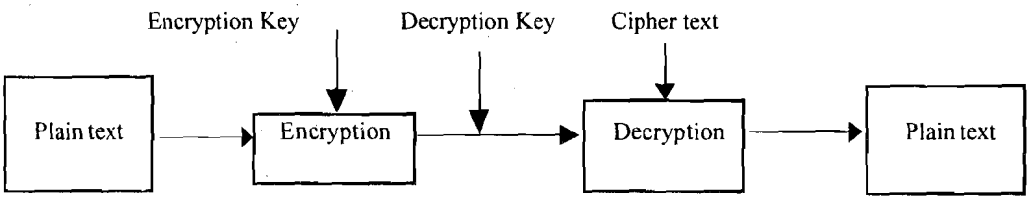


Figure 4: Encryption/ Decryption Mechanism

The performance hit is much more obvious in encryption. If the data packets are encrypted, the information that must be transmitted is bigger, and more bandwidth will be required. Additionally there will be more overheads on devices for performing encryption and decryption.

The computer that is asked to perform encryption and decryption must be able to handle extra workload.

Intrusion Detection System (IDS)

Intrusion Detection Systems are a combination of hardware and software systems that monitor and collect information and analyse it to detect attacks or intrusions. Some IDSs can automatically respond to an intrusion based on collected library of attack signatures. IDSs uses software based scanners, such as an Internet scanner, for vulnerability analysis.

Intrusion detection software builds patterns of normal system usage; triggering an alarm any time when abnormal patterns occur.

What IDS can do?

- By using various techniques it attempt to detection of intrusion into a computer or network by observation of actions, security logs, or audit data.
- Detection of break-ins or attempts via software systems that operate on logs or alert information.
- Cannot stop crime, only prevent and provide evidence for investigations.

Software Controls

- Internal program controls
- OS controls
- Development controls.

Hardware controls

- Locks or blocks limiting access
- Hardware or smart card based encryption
- Devices for user's authentication
- Mechanism to control access to storage media.

Policies

The security policies and procedures must be properly implemented to ensure their proper use.

Physical Controls

- Easy to implement, effective and less costly
- Include locks on doors, guards at entry/exit points
- Backup copies of critical software and data
- Access Control
- Media Control
- Precautions against water and fire damage
- Air conditioning
- Physical site planning that minimizes the risk of natural disasters.

System Security

- International Security Standards: Most computer vendors nowadays adopt international standards into building security facilities into their system.

Computer Virus

- Computer should be equipped with updated virus protection and detection software.
- Virus detection software must check storage drives both internal and external to the system on a regular basis.
- All diskettes and software shall be screened and verified by virus scanner software before being loaded onto the computer system.

Personnel Security

Personnel security is everything involving employees, who are potential elements of breaches of security.

- Hiring them
- Training them
- Monitoring them
- Handling their departure

Why personnel Security?

- Most of the Security breaches are caused by people only like, break-ins, virus generation etc.
- Statistics reveal that the most common perpetrators of significant computer crime are the legitimate users of the computer system.
- Some studies show that over 80% of incidents are due to internal users.

Auditing

Auditing is a tedious process and requires a good eye for details.

- Track everyone who logs on and off the computer system.
- Audit movement of critical files, attempted deletion or access to mission-critical data.
- Some of the common red flags to watch for in auditing are – multiple bad logon attempts, or same account trying to log in from many locations at the same time, and attempted shutdown of critical servers.

It is due to time-consuming process of reading the logs that many companies avoid auditing of log files. The organisation that takes the log files for granted will end up as one that is unable to inform the legal agencies that an incident has really happened.

☞ Check Your Progress 2

1) Identify computer assets in your organisation.

.....

.....

.....

.....

2) Identify threats to assets listed in progress 1 above.

.....

.....

.....

.....

3) Identify the impact of security attack listed in 2 above.

.....

.....

.....

.....

1.7 CRYPTOGRAPHY

A cryptosystem is an algorithm, plus all possible plaintexts, cipher texts, and keys.

A cryptographic algorithm, also called a cipher, is the mathematical function used for encryption (E) and decryption (D). The key is a large number. The range of possible values of the key is called the key space. Both encryption and decryption use this key space.

$E_K[M] = C$

$D_K[C] = M$

or. $D_K[E_K[M]] = M$

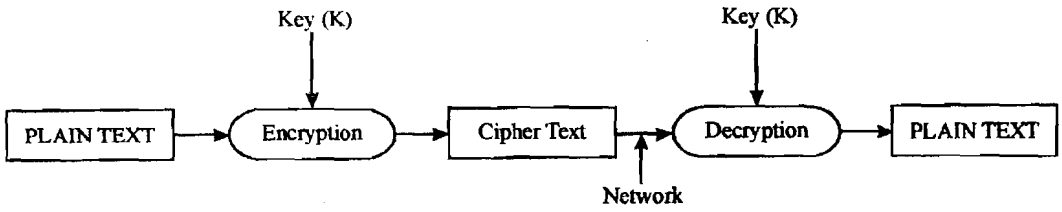


Figure 5: Encryption & Decryption using same key

Sometimes algorithms use a different encryption and decryption key. The encryption key K1 is different from decryption key K2 (Figure 6).

$$E_{K1}[M] = C$$

$$D_{K2}[C] = M$$

$$\text{Or } D_{K2}[E_{K1}[M]] = M$$

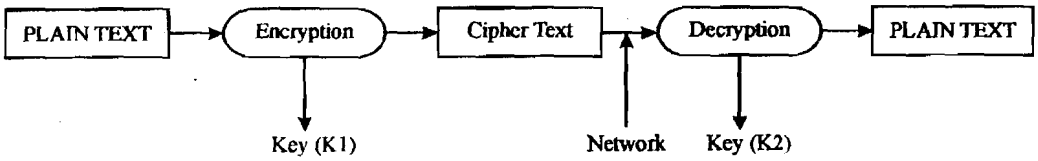


Figure 6: Encryption & Decryption using different keys

There are two general types of key-based algorithms: symmetric and public-key (asymmetric algorithm). The universally accepted modern method of electronic authentication is the one based on asymmetric cryptosystems. This is also known as public key cryptography, and is the basis for creating digital signatures. However rapid advancements and technological changes are challenging the supremacy of digital signatures as the only method of electronic authentication. Biometrics and dynamic signature analysis, among other technologies, are expected to be equally important in the years to come. It is also expected that some of the biometric techniques may prove to be more reliable and less susceptible to compromise than digital signatures. In view of the pace of technological development, no single technology may prevail for a long time as the sole means of electronic authentication.

1.8 INTRUSION DETECTION

ID stands for Intrusion Detection, which is the art of detecting inappropriate, incorrect, or anomalous activity. ID systems that operate on a host to detect malicious activity on that host are called host-based ID systems, and ID systems that operate on network data flows are called network-based ID systems.

Sometimes, a distinction is made between misuse and intrusion detection. The term intrusion is used to describe attacks from the outside; whereas, misuse is used to describe an attack that originates from inside the organisation's network. However, most people don't draw such distinctions.

The most common approaches to ID are statistical anomaly detection and pattern-matching detection.

Increased usage and consequent exposure have led to the need to develop security components for the Web interface architecture. One such component is Intrusion Detection system. Intrusion Detection systems are however complex to implement, especially on large networks, because they generate vast quantities of data and require significant configuration and management. IDS's come in many forms and implementation models. Some rule-based systems rely on preset rules. Anomaly-based systems generate their own baseline overtime by building a database of recorded network usage. When network usage moves outside of the developed pattern, the IDS sounds an alarm.

In addition, IDS can be either host or network based or a combination thereof. A host based IDS is installed on and looks for potential malicious authority on a specific

computer. A network based IDS records network traffic and scans for suspicious activity using sensors and agents installed throughout a network often through a tap off of a hub or a switch with a spanner port. It looks for malicious commandos, repeated failed login attempts, traffic peaking at odd hours or other evidence of possible mischief.

1.9 COMPUTER–SECURITY CLASSIFICATIONS

The "Trusted Computer System Evaluation Criteria (TCSEC or orange book)" is the most widely accepted standard in the industry. The TCSEC model was developed based on a hierarchical model of security classifications.

The classes of systems recognised under the TCSEC are as follows. They are represented in the order of increasing desirability from computer system security point of view.

Class D (Minimal Protection)

A system with a Class D rating does not have to pass any tests to be rated as a class D system.

Class C1 (Discretionary Security Protection)

For a system to have C1 level security, it must provide a separation of users from data. Discretionary access controls need to be available to allow a user to limit access to data. Users must be identified and authenticated.

Class C2 (Controlled Access Protection)

For a system to have C2 level security, a user must be able to protect data so that it is available to only one user at a time. An audit trail that tracks access and attempted access to objects, such as files, must be kept. Further C2 security requires that all the residual data generated in temporary memory or register is erased.

Class B1 (Labeled Security Protection)

Systems at the B1 level of security must have mandatory access control capabilities. Mandatory access controls limit access to objects based on the sensitivity of the information contained in the objects and formal authorisation of subjects to access information. The subject and objects that are controlled must be individually labeled with a security level. Labels must include both hierarchical security level such as "unclassified", "secret", and "top secret", and categories. Discretionary access control must also be present.

Class B2 (Structured Protection)

For a computer system to meet the B2 level of security, there must be a formal security model. Covert channels used to transmit data must be constrained. There must be a verifiable top-level design, and testing must confirm that this design has been implemented. A security officer is designated to implement access control policies.

Class B3 (Security Domains)

The security of systems at B3 level is based on a complete and conceptually simple model. The capability of specifying access protection for each object, and specifying allowed subjects, the access allowed for each, and disallowed subjects must be included. A reference monitor for accessing user's requests and allows or disallows access based on access control policies, must be implemented. The system must be tamper proof and highly resistant to penetration. Auditing must be available for detection of security violations.

Class A1 (Verified Design)

The capabilities of a class A1 system are identical to those of a B3 system. However, the formal model for a class A1 system must be formally verified as secure.

☞ Check Your Progress 3

1) Distinguish between vulnerability and threat.

.....

.....

.....

2) List any three recent computer security failures.

.....

.....

.....

3) Do you currently apply any computer security control measures? If so, what?Against what attacks are you trying to protect?

.....

.....

.....

4) Discuss various security systems and facilities.

.....

.....

.....

5) What is computer-security classification?

.....

.....

.....

6) What do you understand by symmetric and asymmetric cryptography?

.....

.....

.....

1.10 SUMMARY

Computer security attempts to ensure the integrity, confidentiality, and availability of computer system. Computer systems are subject to attacks: hardware, software, and data. These three components and communication equipment associated with the computer constitute the basis of computer security vulnerabilities. Further, the people and systems interested in compromising a system can devise attacks that exploit the vulnerabilities. Four kinds of attacks on a computer system–interception, interruption, modification, and fabrication–have been discussed.

Controls can be applied at the level of the data, the programs, the system, the physical devices, the communication lines, the environment, and the personnel.

1.11 SOLUTIONS/ ANSWERS

Check Your Progress 1

1) The goals of computer security are:

   a) Data integrity

   b) Data confidentiality

   c) Data availability

2) Confidentiality ensures that the information in a computer system and transmitted information are accessible only for reading by authorised parties. This includes printing, displaying, and other forms of disclosure, including simply revealing the existence of an object. And without integrity of data, this is not possible.

Check Your Progress 2

1) This includes hardware, software, data, people related to system operation and management, documentations, and supplies, etc.

2) Threats are of two types: (1) accidental threats, (2) intentional threats.

3) The impact of security attacks could be: (1) infringement of privacy, (2) financial loss, or (3) disruption of activities.

Check Your Progress 3

1) a) A threat is a set of instances that has the capability of causing loss or harm to the computer system. There are many threats to a computer system and can be (a) Human initiated, (b) Computer initiated, and (c) Natural disasters like flood or earthquake. A threat can be accidental or deliberate and the various types of security breaches can be classified as (a) interruption, (b) interception, (c) modification, and (d) fabrication.

   b) A computer system has three valuable components: hardware, software, and data. Vulnerability is a weakness in the system. This weakness may be exploited by threats causing loss/damage or harm to the system. Vulnerability does not cause any harm until exploited. It can be a weakness in: (a) procedures, (b) design, and (c) implementation.

2) "Trusted Computer System Evaluation Criteria (TCSEC or orange book)" is the most widely accepted standard in the industry. The TCSEC model was developed

based on a hierarchical model of security classifications. It includes various classes like Class D, C1, C2, B1,B2, B3, and A1.

3) In the case of symmetric cryptography encryption key is same as the decryption key. But, in asymmetric cryptography, also known as public key cryptography, encryption key is different from the decryption key.

1.12 FURTHER READINGS

1) http://www.mit.gov.in/it-bill.asp Information Technology Act 2000, India.

2) *Cryptography and Network Security, Principles and Practice*, William Stallings –SE, PE.

3) *RSA Security's Official Guide to Cryptography*, Steve Burnett and Stephen Paine – RSA Press.

4) http://www.cca.gov.in Controller of Certifying Authorities, Web Site.

5) *Security in Computer*, Charles P. Pfleeger and Shari Lawrence Pfleeger, Third Edition, Pearson Education.

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*.

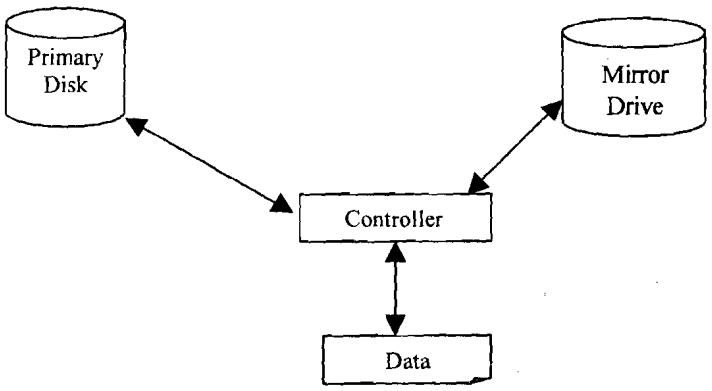


Figure 1: Disk Mirroring

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

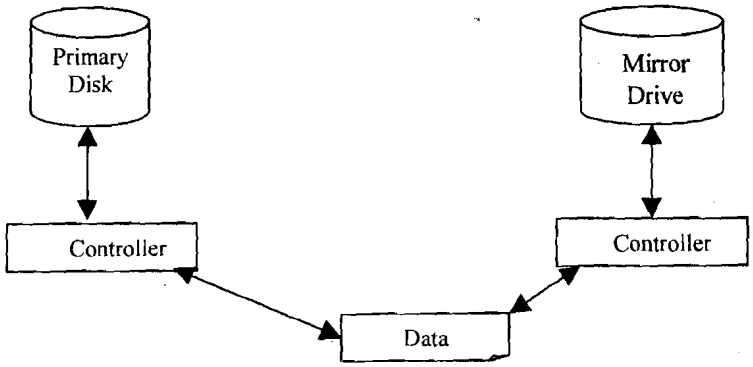


Figure 2: Disk Duplexing

- **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

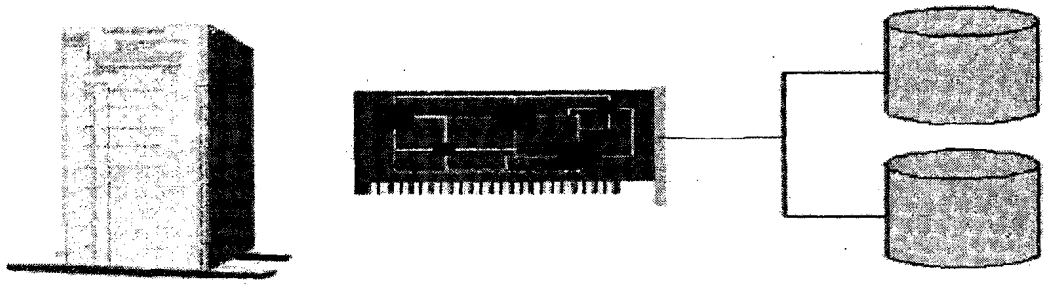


Figure 4: Drive Mirroring

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.

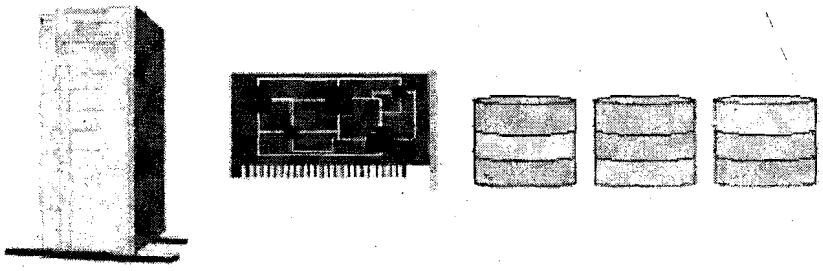


Figure 5: Striping with Party (or RAID 5)

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

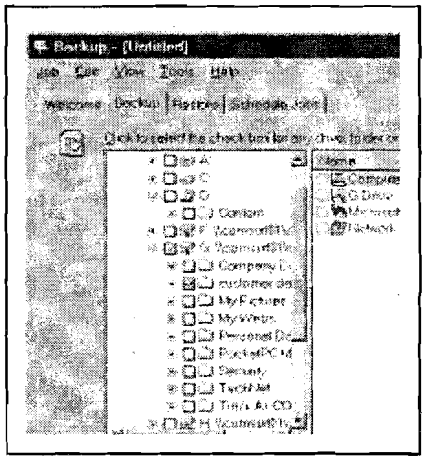


Figure 6: Windows 2000 Backup

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

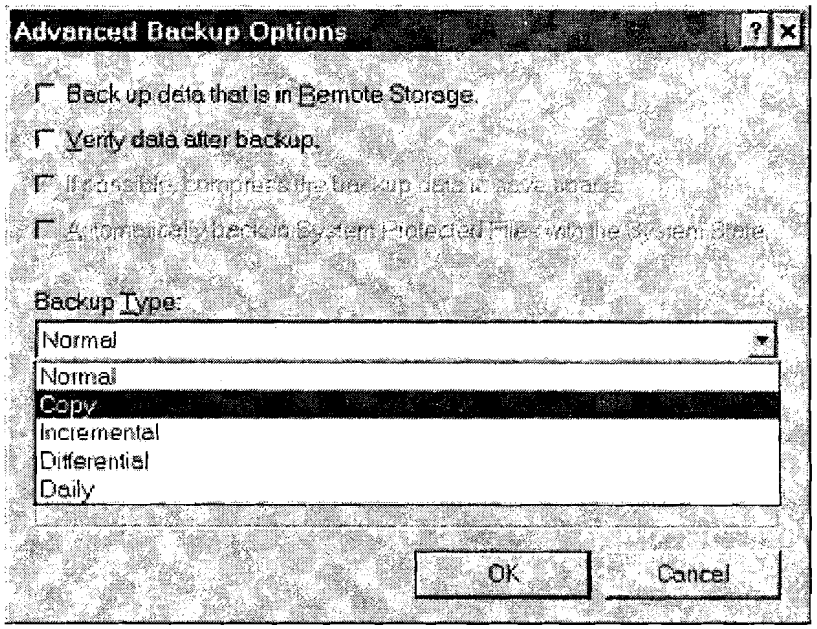


Figure 7: Choosing the Backup Type

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.*

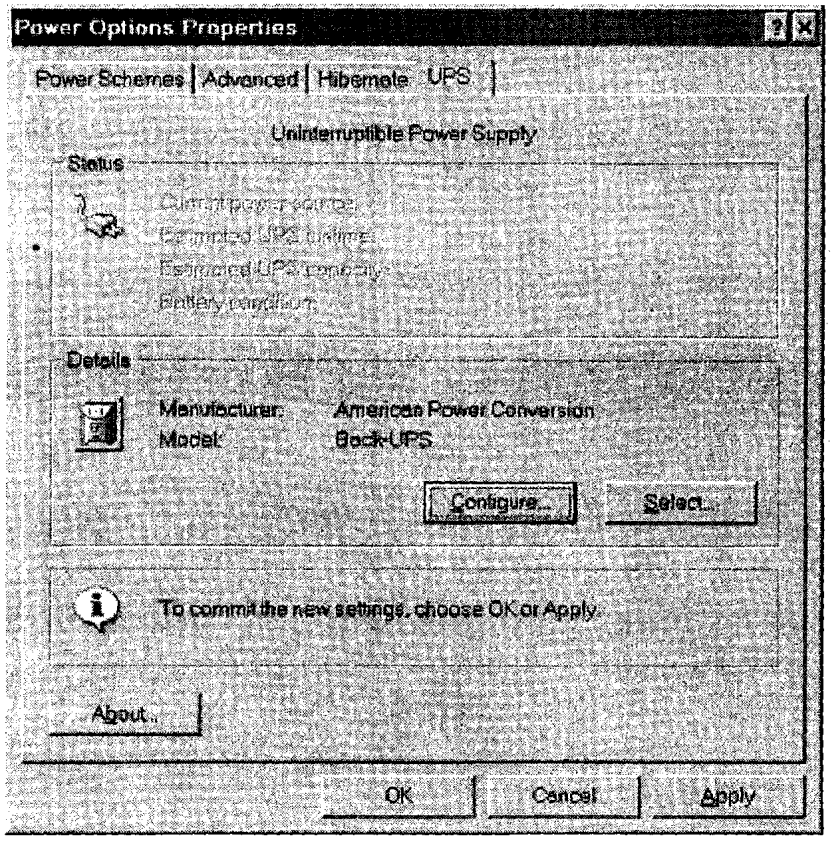


Figure 8: Selecting your UPS in Windows

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

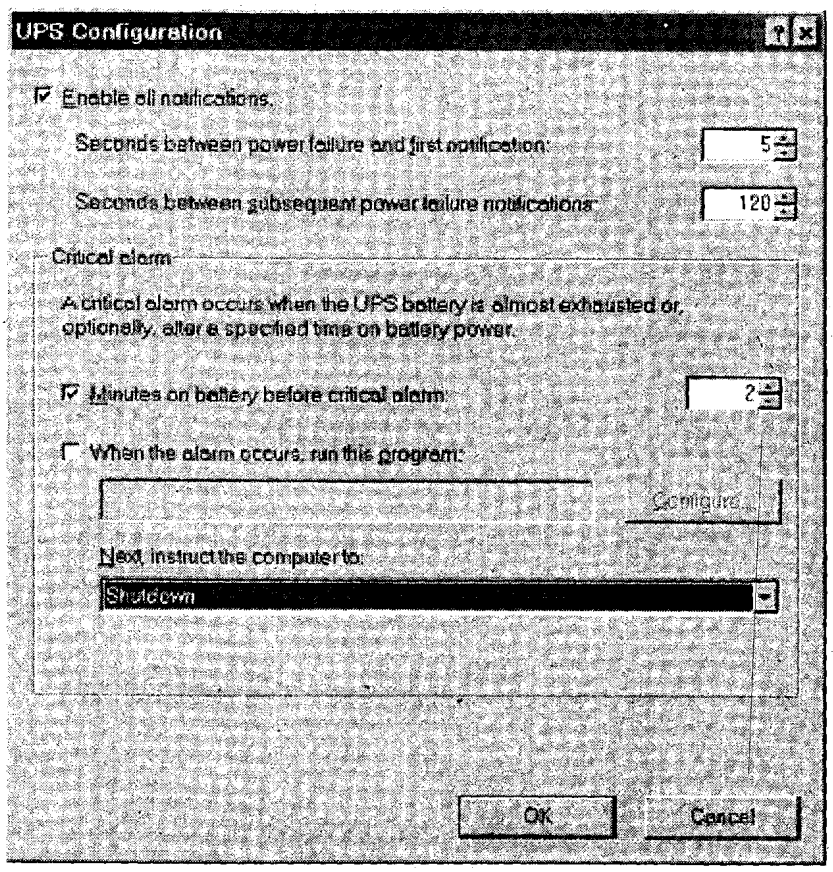


Figure 9: Configuring the UPS

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

UNIT 3 SECURITY AND MANAGEMENT - I

Structure **Page Nos.**

3.0 INTRODUCTION

In this unit we will discuss the concepts and configuration required to secure Microsoft Windows computers and also examine everything from the foundational principles of Windows NT Security Management, up to the advanced issues of securing Windows 2000 machines running Active Directory. The unit address is a broad sweep of concepts of Windows Management Architecture and security related issues: Main Issues in Windows Security; Windows Resource Management; Windows 2000 Operating Systems.

Section 3 of this unit deals with "Main Issues in Windows Security and Management" and it covers the following areas; physical security management, logon security management, user/groups management, Windows NT domain model, domain controllers.

Section 4 of this unit deals with Windows resource security management and it covers areas like; files and folder management, files/folder permissions, printer management and Registry Management.

The most important, section 5, deals with the management of Windows 2000 operating system; Windows 2000 features, active directory, logical structure, physical structure, Windows 2000 DNS, Group Policy etc.

3.1 OBJECTIVES

After going through unut you will be able to learn:

- management of Windows NT system, and
- examine the fundamentals of the Management of Windows 2000 system.

The objective of this unit will be:

- examine the various issues of Management of Windows NT 4.0.
- study and manage Windows NT 4.0 Resources
- examine the Windows 2000 Infrastructure.

3.2 MAIN ISSUES IN WINDOWS SECURITY MANAGEMENT

In this section we will point on main issues in windows security management.

3.2.1 Physical Security Management

The main problem or issue of computer security is unauthorized physical access to a secure computer system and it is breech of computer security. If a computer is in a public area it should not contain any sensitive data.

The following steps should be taken to improve physical or local security: computer BIOS must have a password, and computer should be configured to boot from hard drive and not through floppy or any other external media. In Windows NT Server provides options to control local access or right to log on locally and this adds another layer of security on computer.

3.2.2 Logon Security Management

When a user logs on to a Windows NT machine, he is presented with an onscreen message or notice. This message must clearly state the intended use of the computer system. It is suggested that the banner should not have a greeting, or a welcome message. The main steps for creating a user account are given below:

Creating a User Account

1. Log on as an Administrator.
2. Navigate to: User Manager for Domains.
3. Select User -→ New User.
4. Type user name in the Username Field.

5. **Type your first name in the Password Field.** Please note that passwords are case sensitive.
6. Type the exact same password in the Confirm Password Field.
7. Add this user to the Administrators Group.

Steps for Logon Security

1. Creating a Logon Warning Message
2. In the run option, type Regedit to open the Registry editor.
3. In the Registry Editor navigate to:
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogo.
4. Double-click the LegalNoticeCaption value.
5. In the Value Data entry field, Type Unauthorized Access Warning!! Then press OK
6. Double-click the LegalNoticeText value.
7. Type in the Value Data Entry Field.

   "Unauthorized access to this system is punishable by a fine of Rs 7,500 and/or one year in prison. Use of this system indicates that you have read and agree to this warning".
8. Press OK.
9. Close the Registry Editor.
10. Log off and verify the changes.

In addition to logon security management, you can eliminate the name of the previous user logged onto the system. If the last username is not eliminated, then an intruder or hacker can simply look at the screen, or press [Ctrl][Alt][Del] to find out the previous user. By getting a valid username, the intruder has acquired half of what is required to gain access to the system.

3.2.3 Users and Groups Management

In Windows NT every unique user of the system has a unique user account and this account is provided a Security Identifier or SID at the time when account is used. Windows provides multiple levels of user account with the most powerful user account the Administrator (Or Domain Administrator in a domain environment). The Administrator account has the power to manage all the settings on each system and as a result this is the account that must be properly secured. It is suggested that the Administrator account should not be used for day-to-day work at the network. Network administrators should create a separate account for daily routine activities and the Administrator account should be used only when it is absolutely required.

Permissions for resources can be set for individual users but this is not the most efficient way to manage the security of files and folders. It is for this reason that it is necessary to manage the permissions of resources. The function of groups is to assign users who have similar requirements for the use of resources. In this way you will be able to define access to the group rather than to the individual user.

3.2.4 Managing Local and Global Groups

The Administrator can manage the groups in two ways. The two options are Local Groups and Global Groups. Local Groups apply to a single computer and are used to

control access to resources on the local computer. Global Groups apply to an entire domain, or group of computers.

You can combine groups together, local and global. But the only allowed combination is to put a Global Group into a Local Group. This is accomplished by adding new computers or members to the Local Group, and from the list selecting a Global Group as the member.

3.2.5 Managing User Accounts

When securing the Windows System, the standards regarding user passwords should be followed. It must be ensured that users are not using weak, or easy to guess passwords and there should be no user accounts that have a blank password, and none that have a password that is the same as the username.

Please Note: Windows 95/98 and Windows NT support 14 character passwords and remember this as it may be required for backwards compatibility if you are using Windows 2000.

The Windows System provides the required help to an administrator for managing passwords. In User Manager for Domains (or User Manager on workstations or standalone servers), the administrator can define Account Policies. These account policies provide various options such as: how long a password is good, how long the password must be, and how many failed attempts will cause the account to lockout, often set to 3. It is necessary to have the password change often for high security, and for the system to remember passwords, preventing users from using the same password over and over again. The following steps should be followed for defining the account policies.

Steps for Defining Account Policies for disabling last username option.

1. Disabling the Last Username option
2. In the run box. type Regedit to open the Registry Editor.
3. Navigate to: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon
4. From the drop-down menus choose Edit > New > String Value.
5. Type DontDisplayLastUsername in the Name Field
6. Double-click on your new string.
7. Type 1 in the Value Data entry field, and press OK to close the Edit dialog box.
8. Close the Registry Editor.

Log off and back on again (no need to restart) to verify the changes. Verify that the last user name no longer appears in the logon box.

1. Log on to your Windows NT Server as Administrator.
2. Navigate to: User Manager for Domains.
3. From the drop-down menus select Policies > Account.
4. Halfway down the page select the Account Lockout radio button.
5. Modify the Account Lockout settings to the following:
   a. Lockout: after 5 bad attempts.
   b. Reset count: after 100 minutes.

c. Lockout

d. Duration: Forever (until admin unlocks).

6. Close the Account policy dialog box by pressing OK.
7. Log off as Administrator and try these changes.
8. Log back on as Administrator.
9. Navigate to: User Manager for Domains.
10. Double-click on the user you used above.
11. Verify that the Account Locked Out radio button is checked, and uncheck it. Then press OK.
12. Close User Manager.

It is also necessary to secure the Guest account and this account should never be used in a secure environment. The guest account can be locked down by the following steps:

- Rename the guest account to a difficult - to - guess account name.
- Remove the guest account description.
- Set a very complex 14-character password.
- Change logon hours to never.
- Change the logon to option to a Workstation that is not active.

The concept of user accounts and groups provides an efficient way to manage access to resources, but to define the network itself a larger concept, called the Window NT Domain model, is available.

3.2.6 Windows NT Domain Management

The model of Windows NT Security allows you to control many users, groups, and computers by using a boundary known as a Domain. A server called the Primary Domain Controller (PDC) controls a Domain and there can be only one PDC per domain. But there can be a number of Backup Domain Controllers (BDC) to assist PDC. This Domain model allows for thousands of computers and users under a single management option. When a user logs on to a domain, he is able to access all the computers in the logged domain, with the security of those computers dictating the actual level of permission to objects.

This model also provides for a Single Sign On (SSO) to all resources, that is the user is not required to provide credentials for each computer that s/he wishes to access. While the domain model is useful, it does have limitations: (a) a very large domain would be hard to manage efficiently, and (b) users who are very far apart physically may find a more efficient network experience to have one domain per location.

Regardless of the reason, in order for the network to expand, more than one domain is required. To maintain the SSO across multiple domains a method called trust relationship is used. A trust relationship is an administrative link between two domains. A domain that trusts another domain is called a TRUSTING domain and the other domain is called TRUSTED domain. The TRUSTED domain or Accounts domain holds the user accounts and the TRUSTING domain or RESOURCE domain holds the resources. The trust is only one-way, meaning that if domain A trusts domain B, then domain B does not have to trust domain A. In order to have trust in both directions, two one-way trusts relationship needs to be created. There are four basic domain

models in Windows NT 4.0: (1) the single domain model (no trust created), (2) single master (one Accounts domains (A), one or more Resource domains (R), (3) multiple masters (two or more Accounts domains one or more Resource domain's) shown in *Figure 2*, and (4) complete trust (all domains have direct trusts to all other domain) shown in *Figure 3*.

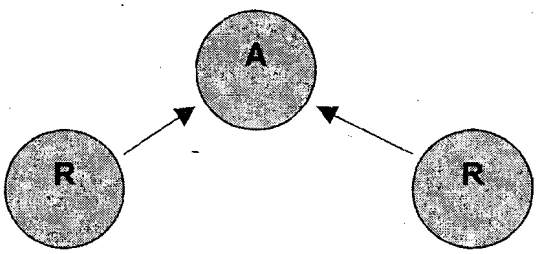


Figure 1: Single Master

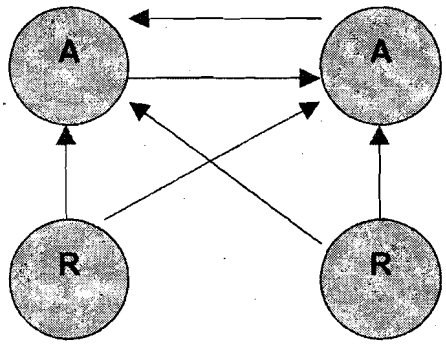


Figure 2: Multiple Master

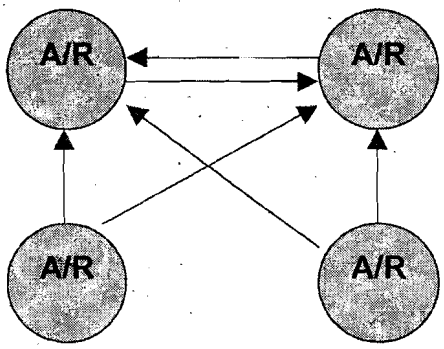


Figure 3: Complete Trust

There is a fifth type of domain structure, but it is not an official model. This type is of a hybrid or mixed layout, shown in *Figure 4* where the trust structure has no specific pattern. In this layout there are some Resource domains as well as some Account domains, spread throughout the network.

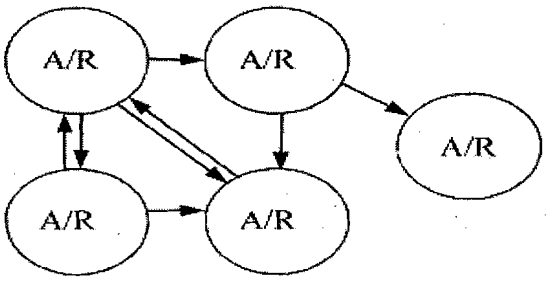


Figure 4: Hybrid or Mixed Layout

☞ **Check Your Progress 1**

1) Create a user account " Testuser" and create a logon warning message:

"Unauthorised access to this system is punishable by a fine of Rs 10,000 and / or one year of imprisonment. Use of this system indicates that you have read and agree to this warning."

.....

.....

.....

.....

2) List the steps for disabling the Last username option.

.....

.....

.....

.....

3.3 DOMAIN CONTROLLER

Windows Server organises groups of computers into domains so that all the machines in a particular domain can share a common database and security policy. Domain controllers are systems that run NT Server and share the centralised directory database that contains user account and security information for a particular domain. When users log on to a particular domain account, the domain controllers authenticate the users username and password, against the information stored in the directory database.

When you perform NT Server installation, you must designate the role that servers will play in a domain. Three choices are available for this role: PDC, BDC, and member server (i.e., a standalone server).

3.3.1 The Primary Domain Controller (PDC)

The first Windows NT Server in the domain is configured as a primary domain controller (PDC). The User Manager for Domains utility is used to maintain user and group information for the domain using the domain security database on the primary controller.

3.3.2 Backup Domain Controllers (BDC)

BDC (Backup Domain Controllers) are the other server after one server has been configured as PDC. BDC stores a copy of the database on the PDC, which is updated periodically to distribute changes made to the main database on the PDC. Such BDC have many advantages:

- If the PDC stops functioning due to a hardware failure, one of the BDC can be promoted to the primary role. Such arrangement provides fault tolerance in the network.

- PDC provides helps in authenticating network logons. When a user logs on to a domain, the logon request can be handled by any PDC or BDC. This provides an automatic mechanism for load distribution and improves logon performance and it is highly useful in domains with large numbers of users.

☞ Check Your Progress 2

1) Fill in the blanks:

   a. The model of Windows NT allows you to control many users, groups, and computers by using a boundary known as a _____.

   b. There can be only _____ PDC per domain. But there can be a number of _____ to assist PDC.

   c. Domain model provides for a _____ to all resources.

   d. A domain that trusts another domain is called a _____ domain and the other domain is called _____ domain.

   e. If PDC stops functioning due to hardware failure, one of the BDC can be promoted to _____

   f. PDC provides help in _____ network logons.

2) What are limitations of the domain model?

.....

.....

.....

2) What do you understand by PDC and BDC?

.....

.....

.....

3.4 WINDOWS RESOURCES SECURITY MANAGEMENT

Files and Folders Management

The following paragraphs explain the management of Windows resources. In Windows there are two levels of security, share level and file level. Share level security is for controlling user access to a resource that has been made available to the network, and functions with any file system on the NT machine. File level security is for controlling user access to an individual file locally on a machine, and functions only on the NTFS file system on an NT machine. The share level permissions on a folder (it cannot be set on a file) have four permissions to choose: No Access, Read, Change, and Full Control. This provides power to an administrator to control access to the shared resource from the minimum of No Access, through to the maximum of Full Control.

The share level permission is helpful in many situations, but when you require further control, or wish to secure resources on the local hard drive, you must use file security. The file level security requires that you must use NTFS file system. When permission is set at the file level, the "Everyone group" has Full Control by default.

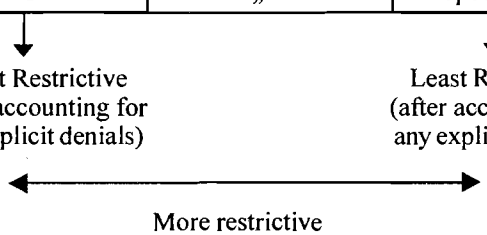
The share level permission could only be applied to a folder; NTFS permissions may be applied to either a folder or a file. Just as you are allowed to set permissions by each user but you can do so by setting the permission for a group to save time and effort, you will normally set permissions by folder, not file, to save time and effort. Setting the file level security one file at a time can take too long on a file server with thousands of files available over the network.

The NTFS file system provides the following permission for resource:

- List - Allows a user to view a field or subdirectory name, but not read the contents of any file or subdirectory.
- No Access - Removes all access rights, and will override any other permission a user may have to this object
- Read - Allows user List permissions, with the added right of reading the contents of a file or subdirectory, and run applications.
- Add - Allows a user the right to add files and subdirectories.
- Read and Add - Allows a user Read permissions, with the added right of adding files and subdirectories to the directory.
- Change - Allows user Read & Add permissions, with the added right of changing data in a file or subdirectory and deleting files and/or subdirectories.
- Full Control - Allows user Change permissions, with the added rights of changing permissions on files and subdirectories and taking ownership of files and Subdirectories.
- Special Access - This permission allows a user to be given access as in *Table 1.*

Table 1 : Assigning Permission for resource

Over the network	**Share permissions**	**NTFS permission local to the machine**	
Access Control List	Corresponding Access Control Entry	Access Control List	Corresponding Access Control Entry
User or Group	No Access	User or Group	No Access
,,		,,	List Holidays
	Read	,,	Add
		,,	Add & Read
		,,	Change
,,	Change	,,	Full Control
,,	Full Control	,,	Special Access



3.5 REGISTRY MANAGEMENT

In older versions of Windows, the Operating System was controlled by multiple files, such as: autoexec.bat, Config.sys, system.ini, and win.ini. In Windows NT, the configuration of the Operating System is stored in what is known as the Registry.

The Registry consists of values, keys, subtree, and hive.

- Values - These contain the information that is stored as part of the Registry. Each value contains three distinct parts: (1) a data type, (2) a name, and (3) a configuration parameter (this contains the actual information).
- Keys (and Sub keys) - These contain the actual Subkeys and values.
- Subtree - These are the highest-level Keys of the Registry. There are five Subtrees in Windows.
- Hive - These are a set of keys, subkeys, and values of the Registry. Each one is stored in its own file in the %systemroot%\System32\Config.

Regedit.exe and regedit32.exe are the two utilities that can be used to manage the REGISTRY. While Regedit.exe provides the ability to view the entire Registry in a single tree, Regedt32.exe on the other hand, allows for managing of individual keys.

3.5.1 Removing Registry Access

The first step to secure Registry is to try to prevent unauthorised users from accessing the Registry. To do this, the operating system files should be installed on an NTFS partition and change the permissions on both the Regedit.exe and the Regedt32.exe so that only members of the Administrators group have Full Control.

3.5.2 Managing Individual Keys

In Registry you can secure individual areas of the Registry as necessary. This option is available in Regedt32.exe which permits you to selectively secure the various keys by using the Security Permissions option. Although the details of securing each key are beyond the scope of this unit, the process is identical to that of securing file resources. You must determine the proper level of access for each key, based on your requirement, and limit permissions accordingly.

3.5.3 Audit Registry Access

After locking down the Registry as per your requirement, you need to make sure that the auditing of critical components of Registry is turned on. This option will help in tracking who accessed the Registry, from where, and when. In order to audit the Registry, the first step is to enable auditing for the computer itself.

The steps for enabling auditing is given below:

1. Logon as Administrators.
2. Go to User Manager for Domains
3. In the Policies menu, select Audit
4. Select Audit These Events to enable these audit choices. Select Failure for the File and Object Access event.
5. Choose OK, and close User Manager for Domains.

There are several options, but for the minimum of registry audits, the Failure for the File and Object Access event is all that is required. Once auditing is turned on for the system itself, you can enable auditing of the Registry. The steps for enabling the auditing registry access is given below:

Steps for enabling the auditing of Registry Access:

1. Log as Administrator
2. Run Regedt32.exe

3. Select the '\Hkey_Local_Machine' Tree

4. Select the Security, Auditing menu option.

5. Add the specific users and/or groups you wish to audit.

6. Choose OK once you have selected all the users and/or groups you wish to add, and confirm your selection.

Some of the Audit events you may wish to use are listed below:

- Write DAC - This audit logs events that try to determine who has access to the key.
- Read Control — This audit logs events that try to determine the owner of a key.
- Delete - This audit logs events that try to delete a key from the Registry.

If you select auditing on all keys for all users this may result in performance hit on the system as it tries to track all these events. Therefore, you should only audit the events you specifically wish to audit. You may view the audited events in the Event Viewer under the Security Log. Events that are audited in the Registry will identify the user, computer, and the event that was audited.

3.6 PRINTER MANAGEMENT

Managing files and folders properly on a Windows machine is just the beginning of setting up the computer's security. Another aspect of computer security is printer management. In Microsoft terminology the printer is a software component, and the hardware device is called the print device. This section will cover this software component in the computer.

Printer permissions are generally overlooked, but in fact it should be taken seriously. If someone has recently purchased an expensive colour laser print device, it should not be used for general print jobs. Print resources are generally the most misused resources in an organisation.

The following four permissions can be set for printers in Windows environment : access, (2) print, (3) manage documents, and (4) full control.

1. No Access -User cannot print to this device or connect to its print queue.

2. Print -User can print documents and manage submitted print jobs, if the owner of those jobs.

3. Manage Documents - Allows a user to manage print jobs, including pausing, restarting, resuming, and deleting queued documents.

4. Full Control -Allows a user to create, manage, and delete printers, as well as all the control of the Manage Documents permission.

The location of the print spooler should not be overlocked. If print documents are sent to the hard drive for processing, and are waiting to be printed, the security of those locations is a big issue. By default this location is in the % systemroot%/systeni32/ spoool folder and, by default that folder has a permission of Everyone Full Control. So, if you have resources that are secured on an NTFS partition, and they are spooled to a FAT folder with lax security, this may become a security breach. You can modify the security spooler location by using "advanced tab" of print server properties.

3.7 MANAGING WINDOWS 2000 OPERATING SYSTEM

In the sub-section we will focus on how to manage windows operating system.

3.7.1 Windows 2000 Features

In Windows 2000 you can create workgroup for multiple to share resources with one another. The workgroup is referred to as peer-to-peer networking, since every machine is equal.

In Windows 2000, a local security database is a list of authorised user accounts and resource access data located on each local computer.

The major advancement in the design of a Windows 2000 is new domain model instead of multiple models of Windows NT 4.0. In this ne new model you still group computers together, but they are controlled differently. In a Windows 2000 domain, you group together computers who share a central directory database. This directory database contains user accounts, security information, service information, and more for the entire domain. Active Directory information includes how each object will interact with other objects in the directory. The Active Directory may start out as a small listing and grow to hold thousands to millions of object listings. This directory forms the database for Active Directory and Active Directory is then known as the Window 2000 directory service. In Active Directory no machine is designated as PDC or BDC instead every system is simply called a Domain Controller. In addition to the information mentioned earlier, the Active Directory holds the information regarding access control. When a user logs on to the network, s/he is authenticated by information that has been stored in the Active Directory. When a user attempts to access an object, the information required to authorise such access is also stored in the Active Directory, and is called the Discretionary Access Control List (DACL). Active Directory objects themselves can be organised into what are known as classes. Classes represent a logical grouping of objects at the discretion of the administrator. Object class examples are: user accounts, computers, omams, groups, an organisation Units (OUs). You also have the ability to create containers, which can hold other objects. Windows 2000 domain is not bounded by location or network configuration, it may be with in a LAN or far apart over a WAN.

3.8 ACTIVE DIRECTORY

Active Directory contains several critical components; these components are logical in nature and have no boundaries. These components are domains, forests, trees, and organisational units (OU). The components of Active Directory that are more physical in nature are the domain controllers and sites, the physical IP subnets of the network. The functionality of Active Directory separates the logical from the physical network structure.

3.8.1 Logical Structure

Active Directory has the ability to build a logical network that mirrors the logical structure of the organisation. As logical structure is more intuitive to users they are able to find and identify resources by logical name, without having to have any knowledge of the physical layout of the network.

The main component behind the structure of Active Directory is the Domain. Active Directory consists of at least, but not limited to, one domain. Microsoft has termed the objects stored inside a domain as interesting objects. These interesting objects are defined as those objects which a user requires in the course of doing their job function. Examples of interesting objects could be printers, databases, email addresses, other

users, and more. Each domain holds information about all the objects in the domain, and only those objects that belong to the domain. Domains are allowed to span one or more physical locations.

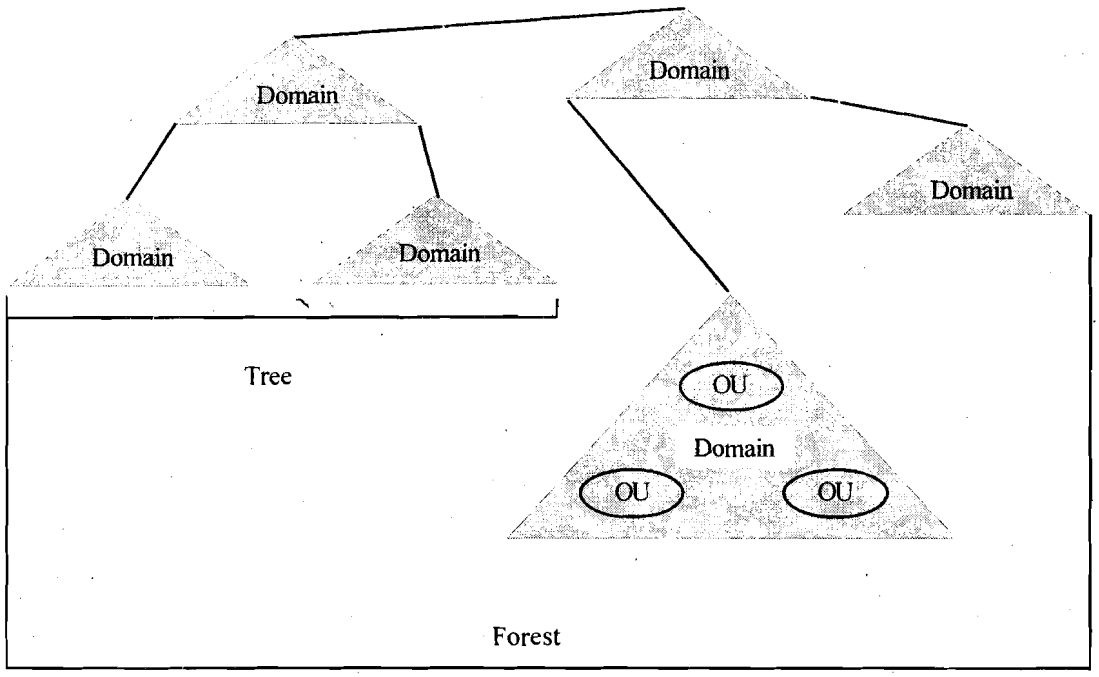


Figure 5 : Logical network layout of a Windows 2000 Active Directory

The domain is used as a boundary by which security controls can be implemented. The Access Control List (ACL) is used to regulate specific access to domain objects, such as shared folders, for defined users. The ACL contains the permissions that are used to grant or deny access for an object, such as a user or group to another object, such as a file, folder, or printer. In the domain it can be called Organisational Units or OUs. An OU is a local holder that is used to further mirror the logical structure of the organisation. An au can contain users, groups, files, folders, printers, and even other OUs from the same domain. Every domain in the network can have a unique OU configuration; as there is no dependency on other domains. Permissions can be granted to an OU as desired. It is possible to assign permissions to each OU, but not required. If there is a permission that you wish all OUs to use in the network, you may assign it to the parent OU of the domain, as the default structure is to allow child objects to inherit permissions from their parent within the Active Directory.

A new concept in Windows 2000 is that of forests and trees *(Figure* 5). A tree is a logical structure created by the network design team of one or more Windows 2000 domains that share a name space. The domains fall in a hierarchical structure and follow the DNS naming standards. A forest in the Windows 2000 Active Directory structure is a collection of completely independent domain trees. These independent trees are tied together with a trust. Each tree in the forest maintains its DNS name system, and there is no requirement for any similar namespace from one tree to another. Each domain functions on its own, but the logical connection of the forest enables organisation wide communication on the network. The implementation of Trust in a Windows 2000 Active Directory network is different from Windows NT 4.0. In Windows 2000 all trusts between domains are called two-way transitive trusts. These trusts, based on Kerberos v5 (a security technique) are created automatically when a new domain is added to the tree. The domain that started the tree is considered the root domain, and each subsequent domain's root will form a Two-Way Transitive trust upon joining.

In the event that older Windows machines are on the network, such as a Windows NT 4.0 machine, a specific trust can be created. This is called an explicit one-way trust such as and it is non-transitive and in this way a Windows 2000 network, running Active Directory, can have communications with an older Windows NT 4.0 Domain. You also have the option of manually creating trusts such as this, so as to connect two Windows 2000 domains that are far down the trees of different forests to improve ? communication speed.

3.8.2 Physical Structure

The majority of the design and implementation of the Active Directory network is on the logical side, but the physical side must be equally addressed. The main components ? of the physical side of Active Directory are sites and the domain controllers.

The site, as defined by Microsoft, "is a combination of one or more Internet Protocol (IP) subnets connected by a highly reliable and fast link to localise as much network traffic as possible." A fast link is reached when the connection speed is at least 512 Kbps. Therefore, the Site is designed to mirror the physical structure of a network, and mayor may not be made up of different IP subnets.

Remember that the domain is designed to mirror the logical needs of the network, and apply that same logic to designing a network using physical aspects. There is no correlation between the site and the domain. It is possible to have multiple domains in a Site, and it is possible to have multiple sites for one domain. A site is also not part of the DNS namespace, which means that when browsing/exploring the directory, you will see user and computer accounts managed by domain and/or OU, but not by site. A site contains only computer objects, and objects relevant to the connection and replication from one site to another.

The other physical component of Active Directory is the actual Domain Controllers (DC) and these machines, which must be running Windows 2000 Server, each have an exact replica of the domain directory. When a change is made on a DC that has an effect on the Active Directory, all other DCs will receive this replicated change. Because any domain controller can authenticate a user to the network, each controller is required to have this directory. Therefore, each DC stores a copy of Active Directory information that is relevant to that domain. Each DC replicates changes, at admin-defined intervals, to all the other DCs to ensure a consistent view of the network at all time? Each DC replicates critical changes to all the other DCs immediately and each DC is able to authenticate user logon requests.

3.9 WINDOWS 2000 DNS MANAGEMENT

For the Active Directory to function, DNS must be running for the network. The implementation of the; DNS namespace will form the foundation on which the Active Directory namespace is created.

A new feature of Windows 2000 is Dynamic DNS (DDNS) which allows clients to receive their IP addresses automatically via a DHCP server and registered with the network. With a DDNS server, the client's machine will automatically communicate with the server, announcing its name and address combination, and will update its DNS information without user information. The advantages of running DNS in a network is the ability to eliminate other protocols and services that may be running to locate resources. For example, the Windows Internet Name Service (WINS) of Windows NT 4.0 is not required, and the use of Net BEUI (Net BIOS Extended User Inferface) as a communication protocol is no longer required.

3.10 MANAGING GROUP POLICY

The final component of the Windows 2000 infrastructur is group policy. A group policy is a logical grouping of user and computer settings that can be inter-connected to computers, domains, OUs, and sites in order to manage a user's desktop environment. For example, a Group Policy is a method of removing objects from the Start Menu.

Group policy consists of GPO (Group Policy Object) and the GPO is then responsible for controlling the application of the policy to Active Directory objects. Once a GPO is configured, it is applied to the AD (Active Directory) object as assigned, and by default the policy will affect all the computers that are in the AD object. The policy can be implemented on all the computers or apply filter how the policy will be implemented for computers and us"ers. The filtering will use Access Control Lists (ACLs), as prepared by you.

Some of the rules for applying a GPO are as follows: a GPO may be associated with more than one domain, a GPO may be associated with more than one OU, A domain may be associated with more than one GPO, and an OU may be associated with more than one GPO. In this section, you have noticed that you are allowed the maximum flexibility in GPO Implememanon. However, Derore getting mto me Implememanon, you must take a step back and look into the GPO itself in more detail.

Policies Options

To configure a GPO open Group Policy Editor via the Microsoft Management Console (MMC). In Group Policy Editor you are provided two options; Users Setting, and Computer Setting. In this you will be able to create the GPO as per your requirements.

In the Computer Settings directory you have the option to manage the behaviour of the a operating system, account policies, IP security policies, etc. The options will be effective once the computer gets restarted.)

The User Settings directory gives the option to manage behaviour that is unique to the user, such as Desktop settings, Control Panel settings, Start Menu settings, etc. These options will be effective once the user logs on to the computer.

Once you create and edit a GPO, it must be enforced to have any impact on the .network and there can be GPOs on Sites, Domains, and OUs. The order of implementation is critical to proper GPO deployment.

The first GPO that is processed is the called Local GPO. Every Windows 2000 computer has a GPO stored locally. However, it is not practical to implement custom configurations on each machine in the network, so often administrators move right past the Local GPO.

After the processing of the Local GPO, the Site GPO is implemented. Since there can be multiple GPOs for one site, it is the administrator's job to deflne the order of .implementation by configuring the Site Properties. After processing the Site GPO, the .Domain GPO is implemented. Just as there can be multiple GPOs for a Site, there can be multiple GPOs for a Domain, so the administrator must take care to define the order .of implementation in this case also.

The last GPO to be processed is the OU. As in the other implementations, more than one GPO may be present for the OU, and as such the administrator is required 10 of; properly plan and implement the GPOs as per the requirements.

In every section with more than one GPO, the place to make the modifications to the order is in the properties of the Site, Domain, or OU (the only exception being the Local GPO). When in the properties of the Site, for example, the GPOs are listed, and the option to move them up or down is present, the system will process the GPOs with the highest on the list having the highest priority, taking precedence over GPOs that are lower down on the list.

The implementation order of the GPOs is critical for the security and management of a Windows 2000 network. By seeing at the implementation order, you can identify that if a Site GPO were to define a password age of 45 days, and a Domain GPO were to define a password age of 30 days, that the final password age would be 30 days, as that GPO was processed last.

☞ **Check Your Progress 3**

1) What is Active Directory?

.....

.....

.....

2) How will you secure guest account?

.....

... .

.....

3) What do you understand by Windows 2000 DNS?

.....

.....

.....

3.11 SUMMARY

This unit describes the broad concepts of Windows Architecture Management and security related issues: Main Issues in Windows Security Management; Windows Resource Management; Windows 2000 Operating Systems. Windows Security specially focuses on Windows NT Management and it covers the areas such as physical security management, logon management, user/groups management, Windows NT domain management, domain controllers. Windows resource management includes areas like: files and folder management, files/folder permissions, printer management, and Registry management. Further, the unit also discusses about the improvement that has been taken up in Windows Architecture, Management with the Management Windows 2000 operating system; Windows 2000 features, active directory, logical structure, physical structure, Windows 2000 DNS management, Group Policy etc. This unit provides detailed concepts and configuration required for management of Microsoft Windows computers and you will be able to examine everything from the foundational principles of Windows NT Management, up to the advanced issues of securing Windows 2000 machines running Active Directory.

3.12 SOLUTIONS/ ANSWERS

Check Your Progress 1

1) • Creating a Logon Warning Message

• In the run option, type Regedit to open the Registry editor.

- In the Registry Editor navigate to:

  HKEY _LOCAL_MACHINE\SOFTW ARE\Microsoft\ WindowsNT\ CurrentV ersion\ Winlogo.5

- Double-click the LegalNoticeCaption value.
- In the Value Data entry field, Type Unauthorised Access Warning!! Then press OK.
- Double-click the LegalNoticeText value.
- Type in the Value Data Entry Field.

  "Unauthorised access to this system is punishable by a fme of Rs 10,000 and / or on , year of imprisonment. Use of this system indicates that you have read and agree to this warning". Press OK.

- Close the Registry Editor.
- Log off and verify the changes :
- Disabling the Last Usemame option
- In the run box. type Regedit to open the Registry Editor.
- Navigate to

  HKEY _LOCAL_MACHINE\SOFTW ARE\Mlcrosoft\ Windows NT\Current Version\Winlogon.

- From the drop-down menus choose Edit> New> String Value.
- Type DontDisplayLastUsemame in the Name Field.
- Double-click on your new string.
- Type 1 in the Value Data entry field, and press OK to close the Edit dialog box.
- Close the Registry Editor.

Check Your Progress 2

1) a) Domain, (b) one, BDC (c) Single Sign On (SSO), (d) TRUSTING, TRUSTED, (e) PDC, (f) authenticating.

2) a) A very large domain would be hard to manage lefficiently, and (b) users who are very far apart physically may find a more efficien\ .network experience to have one domain per location.

3) Primary domain controller and Secondary Domain Controller.

Check Your Progress 3

1) You group together computers who share a central directory database. This directory database contains user accounts, security information, service information, and more for the entire domain.

2) The guest account can be lock down by the following steps:

   - Rename the guest account to a difficult to-guess account name.
   - Remove the guest account description.
   - Set a very complex 14-character password.
   - Change logon hours to never.
   - Change the logon to option to a Workstation that is not active.

3) Windows 2000 is Dynamic DNS (DDNS) and DDNS allows clients, which receive their IP addresses automatically via a DHCP server to have their name IP address registered with the network.

3.13 FURTHER READINGS

1. *Cryptography and Network Security, Principles and Practice,* William Stallings - SE,PE.

2. *Security in Computer,* Charles P. Pfleeger and Shari Lawrence Pfleeger, Third Edition, Pearson Education.

3. *Windows 2000 Commands* by Aleen Frisch.

4. Microsoft Web Site ht!l1://www.microsoft.com.

UNIT 4 SECURITY AND MANAGEMENT - II

Structure **Page Nos.**

4.0 INTRODUCTION

This unit will introduce you to the concepts and configuration required for the management Microsoft Windows computers and you will be able to examine everything from the foundational principles of Windows 2000 security, up to the advanced issues of securing windows 2000 machines running Active Directory.

This unit covers in detail the various security methods that can be implemented in windows 2000 architecture. The unit addresses management of Windows 2000 system: Authentication (section 3); users and group security (section 4); resource security (section 5); windows network security (section 6); and encrypting file system (section 7). The section 3 of this unit deals with windows 2000 user authentication management and it covers the following areas; Subsystems components, and kerberos.

The section 4 of this unit deals with the users and group security management and it covers the topics like; configuring users accounts, windows 2000 groups (default group types, local groups, global groups, group policies etc.), security configuration tools, and configuration management and analysis tools.

The section 5 deals with resource security management and it covers the areas like; files and folder management, files/folder permissions, inheritance and propagation, moving data and permissions, shared resources, null session, printer management, and Registry management.

Section 6 the most important deals with the network management; NAT, ICS, RRAS, RAS, IAS, and IPSec are covered in this section.

The section 7 deals with encrypting file system (EFS), data recovery and EFS cryptography.

4.1 OBJECTIVES

After going through this unit you will be able to:

- learn windows 2000 authentication;
- user and group management;
- resource management;
- EFS Management; and
- windows network management.

Objectives of this unit are: Examine the basics of user authentication in Windows 2000, learn to manage User and Group Options in Windows 2000, manage and configure security options on Windows 2000 Resources, Examine the methods or management network communications in Windows 2000 Examine and configure EFS on Windows 2000.

4.2 USER AUTHENTICATION MANAGEMENT

Despite all the advancements and new components of Windows 2000, a user must be authenticated to access resources on the network. Windows 2000 can use the following for authentication: Kerberos, NTLM, RADIUS, SSL, Smart Cards, and more.

Windows 2000 uses the Security Support Interface (SPPI) to allow for these methods of authentication. The SPPI functions as a interface between the user applications,

such as the Web Browser, and the authentication method, such as NTLM or Kerberos. An application developer need not create an application for each type of authentication possible, but create one that can communicate with SPPI.

Although the SPPI plays an important function in the authentication of users with no options for configuration or management involved in the SPPI. It simply performs its job of connecting authentication requests to the authentication provided by the system.

The administrator is involved more with Security Architecture of Windows 2000, which comprises of parts of both the Operating System and Active Directory. For example, in the Active Directory are the stored account information and policy settings, while in the Operating System is the security process that is and information regarding trusts to and from other areas of the network

If the Windows 2000 is installed in mixed mode, means that there can be both Windows NT 4.0 BDCs and Windows 2000 domain controllers present. This allows for maximum communication options over the network, but it is not the most secure environment. The reason behind this is an issue is that an older networking server, called LAN Manager, used the LAN Manager (LM) protocol for authentication and this protocol has weak security. Windows 9x and NT accepted LM authentication, and this is where the weakness lies and a password can be broken into 7-character pieces and cracked individually. Therefore, even though a 14-character password was implemented, the program that is trying to crack the password is cracking two 7-character blocks at once. The implementation of LM in Windows NT requires the system to not only accept LM authentication, but to store a copy of the LM version of the password in the Registry. Attackers will go after the LM password since they will almost match the NT password.

Microsoft addressed the issue with the default NTLM was to develop and release NTLMv2. There were several increases in the security provided by implementing NTLMv2; the key, or password, was now a 128-bit value, which will take much longer to crack, and MD5 (Message Digest 5) was used to verify the integrity of messages. In order for Windows NT 4.0 machines to implement NTLMv2 they must use Service Pack 4 or greater. If all your clients support NTLMv2, you may configure your Windows 2000 clients to do so also. This may be defined by creating a GPO for an OU that holds all the machines that must use NTLMv2. Then configure the response type, as per your network, in the Security Options, under Computer Configuration, in the Group Policy Editor.

4.2.1 Subsystem Components Management

The logon information is stored in the local Registry on a stand-alone machine or a machine that is part of the workgroup. The Windows 2000 logon process is the same as the Windows NT 4.0 logon process for a stand-alone machine and the Registry stores the user account data in the Security Accounts Manager (SAM). The SAM is used in NT 4.0 to store all user account information, and in Windows 2000 is what is used to store local user account information. But, if a Windows 2000 Server is promoted to be a Domain Controller, the local SAM is no longer accessible. The process for when a user tries to access a local resource is as follows: (1) the user account info is given to the Local Security Authority (LSA). The LSA is what creates the access tokens, provides an interactive environment for user authentication, controls the local security policy, and sends authentication requests to NTLM or Kerberos, as required, (2) the LSA gives the authentication request to NT LAN Manager (NTLM), and (3) the user request for the resource is validated by the Security Reference Monitor (SRM). The SRM performs the actual checks on user permissions to access objects.

4.2.2 Kerberos Management

In Windows 2000 no action is required to implement Kerberos. Kerberos will be used by default to authenticate network clients (with Windows 2000) logging onto a Windows 2000 domain.

Kerberos is an IETF standard used for authentication and the Massachusetts Institute of Technology (MIT) developed it during the 1980s. It is considered to be a secure method, and has been implemented in Operating Systems before the Windows 2000 implementation. There is a bit of controversy in the method used in Windows systems as it varies slightly from the standard created by MIT. However, it should be noted that Windows 2000 is able to intemperate with non-Windows 2000 machines running Kerberos.

When a user the log on process by entering his credentials, Windows will contact an Active Directory domain controller, and locate the Kerberos Key Distribution Center (KDC). An Authentication Server (AS) performs the actual authentication. The KDC responds by issuing a Ticket Granting Ticket (TGT) to the authenticated user. The TGT contains identification information about this user to various servers on the network, and is used to gain further access in the network.

After the user account has been authenticated, the TGT is used to request further Kerberos tickets in order to access network services. The machine that provides the tickets for the network resources to the authenticated client is known as a Ticket Granting Server (TGS).

The benefits to end-users of a network running Kerberos are that a Single Sign On (SSO) will be maintained and the users are not required to authenticate with each resource they wish to access in the network, and since Trusts in Windows 2000 are transitive, once a user logs on to one domain user, s/he will have access to the other domains of the network. Another key benefit of Kerberos is that it has a mechanism for verifying the identity of the user, not just authentication. This means that in a Kerberos network, if a message says it came from User X, you can be very confident it did indeed come from User X.

4.3 USERS AND GROUP MANAGEMENT

In earlier sections we examined the infrastructure of Windows 2000, including the concepts relating to the Group Policy. The following sections builds off those foundational issues, introducing users and groups into the network.

4.3.1 Configuring User Accounts

The focal point of Windows system is the users and without users being able to access the network, there is no point in having a network. There are two basic types of user accounts that may be created in Windows 2000, domain and local. A domain user account has the ability to log on to the network and access authorized resources throughout the domain. A local user account has the ability to log on to a specific computer and access authorized resources on that computer.

The default accounts in Windows 2000 server are the Guest and Administrator. Securing the Guest account and Administrator should happen right away. These steps are as follows: (1) remove the description, (2) disable all logon hours, (3) create a very complex password, (4) and allow the account to only access the network from a nonexistent machine.

4.3.2 Creating Domain User Accounts

The steps for creating domain user accounts are:

a. Open the management console MMC.

b. Open or add the Active Directory Users and Computer Snap-In.

c. Expand domain listing, to view the console tree.

d. In the Action down menu, select option New User.

e. Create new users, user1, user2, user3, user4, etc.

4.3.3 Managing Logon Hours

Once you have created several users, the next step is to restrict logon hours. That means restricting the hours in which a user can logon to the server. The steps are:

a. Open the Active Directory Users and MMC Snap-in

b. Expand domain listing, to view console tree.

c. Select user folder.

d. Double click user1.

e. In the Property Window, choose Account Tab, and select the Logon Hours Option.

f. Limit user1 so that this account can log on to the network during 10 AM to 5 PM during week days (i.e Monday to Friday).

g. Press OK to close the Logon Hours dialog box.

h. Again press OK to close the User1 Property Window.

4.3.4 Managing Expiry Date for a User Account

You can further control the access to network resources by setting a limit or expiry date for a user account.

a. Open Active Directory Users and Computers MMC Snap-In.

b. Expand domain listing to view the console tree.

c. Select user folder.

d. Double click user3 and in pr. erty window select the Account tab.

e. In the Account Expires Option, and select End of option, and enter a expiry date.

f. Press OK.

4.3.5 Windows 2000 Groups Management

While working with Windows 2000 you will most likely want to implement and configure a full Active Directory structure, to gain all the benefits afforded by doing so. However, when you first install a windows 2000 server, it is nothing more than a stand alone server, not even part of a domain, let alone a domain controller.

Once the machine has become a domain controller (by running DCPROMO), as the administrator there are several groups for you to manage. These groups include the Domain Administrators and Domain Users.

There are two group types, a Security Group and a Distribution group. The Distribution Group is used to manage lists, such as email lists.

4.3.6 Default Group Types

On Windows NT 4.0 that groups can be either Global or Local, in Windows 2000 this concepts is expanded. In Windows 2000 the group types are: (1) Domain Local,

(2) Computer Local, (3) Global, and (4) Universal.

Domain Local group is one that may have members from any domain in the network. These groups are only created on Domain Controllers, and can be used to provide resource access throughout the domain. The Computer Local group is used provides access to resources on the local machine only, and cannot be created on a Domain Controller.

Global group is one that combines users who often share network resources use and access needs. Global groups may contain members from the domain in which the group was created.

Universal groups are used in a multi-domain environment where groups of users from different domains have similar resource use and access needs. To implement Universal groups, the network must be running in Native mode, meaning only Windows 2000 computers.

It is also possible to combine groups together, such as Global Groups in Universal Groups. There may be a resource you are trying to control; in this case a Universal group will work for controlling access across the network. You may also place Universal Groups in Domain Local Groups, and control access lo the resource by placing permissions on the Domain Local Group.

These groups can be used for controlling access to resources; both allowing and denying permissions based on your security needs. If you are trying to secure the computer, user, and network environments, you will use Group Policies, as discussed in the previous sections.

Group Policies Management

Two of the issues that must be discussed are the options associated with Policy Inheritance and Overrides. The Group Policy Objects are implemented in the following order: Local GPO, Site GPO, Domain GPO, and OU GPO. And when there is multiple GPOs assigned lo an object such as a Domain that the highest GPO on the list takes priority over the rest of the list. You can change the order of implementation on this list by simply choosing a GPO and pressing the Up or down button to re-order the list as you desire. However, you may need to have further control than what the Up and Down option provides you.

Policy Inheritance

Policy Inheritance is the name of the process of a user or computer inheriting the final policy configuration from multiple policies, depending on where the object may be in the Active Directory hierarchy and configured GPOs. To track the policies that may be implemented as a user logs onto a computer, use the following list: (1) a Computer Policy is enabled when the computer is first turned on, (2) a User Policy is applied, (3) when a user logs onto the system, (4) the Local GPO is applied, (4) the site GPO is applied, (5) the Domain GPO is applied, and (6) the OU GPO is applied.

It is not uncommon for Sites, Domains, and OUs to have more than one GPO configured. It is also not uncommon then for there to be conflicting settings in locations throughout the policies.

No Override

One of the methods for you to manage a GPO implementation is through the No Override option and this option is available on any Site, Domain, or OU GPO. When this option selected, this option means that none of the policy settings in this GPO can be overridden. In the event that more than one GPO is set to No Override, the highest GPO takes priority.

Block Inheritance

The other choice for managing policy implementation is called **Block Policy inheritance** and this choice is also available to any Site, Domain, or OU GPO. This option means that any policy that is higher will not be inherited. Enabling this option will ensure that the settings of the current GPO will be implemented and not the policies of a higher priority policy.

Block Inheritance and No Override options must be used with proper care and if used with incomplete planning can cause serious disruptions to the overall policies that are implemented throughout the organization.

4.3.7 Security Configuration Management Tools

In Windows 2000, there are with a variety of tools and resources for the configuration and management of security options on both individual computers, and the network itself. These tools include The **Security Template Snap-In**, The Security Configuration and Analysis Snap-In, and Secedit.exe. Secedit.exe is a command line tool that can be used for analyzing the security of computers in a domain.

Security Templates

The task of configuring all the options in the GPO can be quite complex at times. To help with defining how the security should be configured for given situations, Microsoft has included Security Templates that can be used in the Group Policy Editor. These templates are .in files and can be opened with a text-editor, for viewing.

Templates are stored in the % system root%\security\templates. These templates can be applied to a GPO, and any user or computer that is controlled by that GPO will implement the security template. A template itself is a set of pre-configured options and Microsoft has included a full set of templates designed to cover most of the standard scenarios that are possible. User can use the default templates as-is, or modify them to suit his requirements. In addition to modifying a template, a user can create his oven template from scratch.

Predefined Security Templates

The list of common Security Templates are given below:

- BASICDC.INF – used to configures default Domain Controller security settings.
- BASICSV.INF – used to configures default Server security settings.
- BASICWK.IN – used to configure default Workstation security settings.
- COMPATWS.INF – used to configures compatible Workstation or Server security settings.
- SECUREDC.INF - This template configures secure Domain Controller security settings.
- SECUREWS.INF - This template configures secure Workstation security settings.
- HISEDC.INF - This template configures highly secure Domain Controller security settings.

- HISECWS.INF — This template configures highly secure Workstation security settings.
- SETUP SECUR1TY.INF - This template configures out of the box default security settings.

There are several general security levels in the templates: Basic, Compatible, Secure, and Highly Secure. The following sections define the general purpose and function of each of the security levels.

Basic templates (BASIC*.INF): These templates allow for an administrator to reverse an earlier implementation of a security configuration and configure Windows 2000 security settings that are not related to user rights.

Compatible templates (COMPAT*.INF) are often only run in a mixed environment. This template configures the system so that local Power Users have security settings that are compatible with Windows NT 4.0 users.

Secure templates (SECURE*.INF) configure security settings for the entire system, but not on files, folders, and Registry keys.

Highly Secure template (HISEC*.INF) is used to secure network communications on Windows 2000 computers and it allows for the highest level of protection on traffic sent to and from Windows 2000 machines. This template requires that a computer configured to use a HISEC template can only communicate with another Windows 2000 computer.

Dedicated Domain Controller (DEDICADC.INF) is used to secure a machine running as a Domain Controller. The reason you may wish to implement this template is that by default the security on a DC is designed to allow for legacy applications, and as such is not as secure as it could be. If your DC is not required to run any of these programs, it is suggested that the Dedicated DC template be implemented.

The final predefined template we will discuss is one that is very important in today's world, but is not included with the other preconfigured templates — the HISECWEB.INF template.

Microsoftat:http;//microsoft.com/default.aspx?scid=kb;en-us;Q316347& This template is discussed in the Microsoft article: "IIS 5: HiSecWeb Potential Risks and the IIS .lookdown Tool (Q3I6347)". The implementation of the HISECWEB.INF template is a requirement for any US 5.0 Web Server that wishes to be locked down.

HISECWEB.INF is designed to configure an US 5.0 machine running the WWW service. Although not in the list of default templates, this can be found and downloaded for free, directly from.

Analysing Password Security Policy of Templates

Open MMC management console, and select Add/Remove Snap-In option. Press Add and add the Security Templates Snap-In. Expand and review the password policy of following templates: Hisecdc, Basicsv, etc.

It is evident from above that the security templates provide a range of configuration. And if default or available templates does not quit fit to your needs, you can simply create a new template altogether.

Creating a Custom Template

a. Open MMC and select Add/Remove Snap-Ins.

b. Click on Add button, and add Security Templates Snap-In.

c. View all templates by expanding Security Templates.

d. Right Click Directory Location (e.g. :\Winnt\Security\Templates) and press New Template.

e. Enter template name: Custom Template.

f. Enter Description: Template for highly secure passwords.

g. Press OK

h. Apply following configuration settings to Custom Template.

- Password History 30 passwords
- Maximum Password age of 15 days and Minimum password age of 3 days.
- Minimum password length 12 characters.
- Account Lockout duration 0 minutes
- Account Lockout Threshold of 4 invalid Logon attempts.
- Reset Account Lockout Counter after 70 minutes.
- Right Click and press Save.

Advance Security Management- Through Security Configuration and Analysis Snap-In Tool.

After creating the policy and making changes in the predefined templates, the templates are applied to the network. As mentioned earlier, templates can be applied (also called Imported) to GPOs and importing a template to a GPO is a straightforward procedure, and uses a tool called **Security Configuration and Analysis Snap-In**.

The Security Configuration and Analysis Snap-In is another of the advances in security management provided by Windows 2000. Through this tool, you are able to implement templates and configure the security of your system. In addition to implementation, this tool allows for a complete security analysis of the operating system.

This tool is compares the security settings of a template to the current configuration of the operating system. During this analysis, this tool will highlight items that are in compliance with the settings with a green checkmark, and highlight those items that are not in compliance with a red X. Implementing the security configuration with an analysis tool is a time consuming process.

Steps are:

a. Open MMC and select Add/Remove Snap-Ins.

b. Press Add button, and add Security Configuration and Analysis Snap-Ins.

c. Right Click Security Configuration and Analysis Snap-Ins and select open database.

d. Open Password_Check.sdb.

e. Select your earlier created Custom Template, and press open.

f. Right Click Security Configuration and Analysis Snap-In and choose Analyze Computer Now and press OK.

g. Right Click Security Configuration and Analysis Snap_ins and examine whether or not your system is up to policies in respect of passwords.

Implementing a Template

a. Open MMC, Right Click Security Configuration and Analysis Snap_ins, and click on Configure Computer Now.

b. Press OK. This process will take several minutes and no message will be displayed.

c. Run the analysis again to confirm the configuration.

☞ Check Your Progress 1

1) State True or False T☐ F☐

a. Kerberos is an IETF standard used for privacy. ☐

b. SPPI is Server Support Interface. ☐

c. The SPPI functions as a interface between the user applications, such as the Web Browser, and the authentication method, such as NTLM or Kerberos. ☐

d. MD5 is Mirror Domain 5. ☐

2) Name various methods of authentication available in windows operating system.

.....

.....

.....

3) Describe kerberos management in windows operating system.

.....

.....

.....

4.4 RESOURCE MANAGEMENT

In this section we are highlighting resource management related issues.

4.4.1 Files and Folder Management

Windows NT 4.0 had the ability to work with only FAT and NTFS file systems, Windows 2000 can also work with FAT32. Further, NTFS should be used for Windows Security Options. NTFS in Windows 2000, technically called NTFS version 5, is required as an administrator wishes to use Active Directory, Domains, and the advanced file security that is provided. Further, the addition of file encryption and disk quotas require NTFS. It is suggested that all partitions that are still running FAT or FAT32 be converted to NTFS in order to effectively secure Windows 2000 resources. If you need to convert a partition to NTFS, the command is (using the C:\ drive as the example): convert volume /FS: NTFS /C. Any new partitions either created or converted to NTFS will, by default, allow everyone group Full Control access. As this includes the Guest and Anonymous accounts, strict security must be implemented before user accounts, which are able to access the system, are added.

In Windows 2000 some additional steps have been added to prevent users from making changes to the system files of Windows itself. Those changes are to hide the folders in the Winnt folder and the System32 folder by default. However, a quick click on the Show File option and all is revealed. There is a built-in mechanism that is working to keep system files from being modified, called the Windows File Protection (WFP) system, and its job is to ensure that system files installed during the setup of Windows are not deleted or overwritten. Only files that have been digitally signed by Microsoft will be able to make these changes.

4.4.2 Files and Folder Permissions

To view permissions, Right-click the object, Select properties, and view the information on the Security tab. One can view more detailed data in advanced option. File permissions are different in Windows 2000 over NT 4.0. Some of the File Permissions available are defined in the following list:

- Traverse Folder/Execute File: The Traverse Folder (Applied to folders only) permission manages a users ability to move "through" a folder to reach other files and folders, regardless of the permissions on the folder. The Execute File (Applied to files only) permission manages a users ability to run program files.
- List Folder/Read Data: The List Folder (Applied to folders only) permission manages a users ability to view file names and folder names. The Read Data permission manages a users ability to read files. (Applied to files only).
- Create Folders/Append Data: The Create Folders (Applied to folders only) permission manages a users ability to create folders within a folder. The Append Data (Applied to files only) permission manages a user's ability to make changes to the end of a file.
- Create Files/Write Data; The Create Files (Applied to folders only) permission manages a user's ability to create files within a folder. The Write Data (Applied to files only) permission manages a user's ability to modify and/or overwrite a file.
- Delete: This permission manages a user's ability to delete a file or a folder.
- Read Permissions: This permission manages a user's ability to read the permissions of a file or a folder.
- Change Permissions: This permission manages a user's ability to change the permissions of a file or a folder.
- Take Ownership: This permission manages a user's ability to take ownership of a file or folder.
- Read Attributes: This permission manages a user's ability to read the attributes of a file or folder.
- Write Attributes: This permission manages a user's ability to modify the attributes of a file or folder.

	Read (Display Data, attributes, owner, pemissions)	Executive (run or execute the file or files in the folder)	Write (to the folder or to the file or change the file attribute)	Delete (the directory or file)	Change Permisson (i.e., the permission to change permissions)	Take Ownership	
FOLDER SECURITY	R	X	W	D	P	O	**FILE SECURITY**
No Access							No Access
List Folder	*	*					
Read	* *	* *					Read
Add		*	*				
Add & Read	*	*	*				
Change	*	*	*	*	*	*	Change
Full Contro	*	*	*	*	*	*	Full Control
Special Access	? ?	? ?	? ?	? ?	? ?	? ?	Special Access

Figure 1: Files and Folder Permissions

These permissions alone are not considered to allow or deny access; the administrator must define on each object. It is not required to specify each of these unique permissions when securing resources. User will most likely use the defined permissions of: Full Control, Modify, Read and Execute, List Folder Contents, Read, and Write. The specific abilities of each of these Permissions are defined in the chart shown in *Figure 1.*

When you apply the Read permission, for example, to a folder, the folder gets the List Folder / Read Data, Read Attributes, and Read Extended Attributes. NTFS file permissions are similar, with the difference of no List Folder Contents as an option, as the permissions are applying to a file.

4.4.3 Inheritances and Propagation

When a user creates a new file, this new file will inherit the permissions of its parent folder, or parent partition on a root level folder. Therefore, if a parent folder is set: Everyone Modify, the file you create in that folder will have everyone modify as its permissions. User can alter this behaviour, create a folder apply the permissions to the This Folder Only option, which means that new data created in the folder will not inherit the permissions of the folder and new objects will inherit the permission that is set one level higher. Therefore, if you have a folder D:\Secure\Self, and this folder has had permissions applied to it only, when you create a file D:\Secure\Self\test.txt, this file will inherit its permissions from the D:\Secure object.

User can also block the inheritance of permissions by clearing the Allow Inheritable Permissions from Parent to Propagate to this Object option on the Security tab of the Properties windows for an object. When you clear this option, you will be presented with three options: (1) Copy the permissions that this object has inherited, (2) Remove all permissions except for those that have been specifically applied, and (3) Cancel the operation and keep the permissions as they were.

The process of configuring/setting permissions in Windows 2000 is similar to that of Windows NT 4.0, with the exception that you will specifically allow or deny access. If you wish to give a user or a group what was called No Access in Windows NT, you would, in Windows 2000, give that user or group Deny to the Full Control permission.

The attacker can get around your NTFS security, if they are able to get physical access to the computer by using MS-DOS etc. User may think that using DOS will not have an effect on any files that are on an NTFS partition, and that DOS will not even be able to recognise the NTFS partition. In most situations this is true; however there are tools and utilities on the market that are designed to access NTFS from DOS. One of the most common of these tools is simply called NTFSDOS.

Steps for assigning permissions

a. Open Windows Explorer, and select any NTFS partition.

b. Create a new folder, called protected_folder and right click this folder and select properties.

c. Select Security tab and clear the Allow inheritable permissions from parent to propagate to this folder, and choose copy option.

d. Add the user3 and give this account Deny- Full Control permission.

e. Add the user2 and give this account Allow- Modify permission.

f. Add the user4 and give this account Allow- Read and Execute permission.

g. Press Advance button and select User1 and press View/Edit.

h. Modify security settings to Apply onto: This folder only (i.e., protected_folder).

4.4.4 Moving Data and Permission

When data /files are moved from one folder to the another, what will happen to the security permissions that were set to secure these files. When files that are secured on an NTFS partition, how their security settings may be altered if those files are moved. In other words, if a file is defined as having everyone — allow — Read & Execute permissions, what will happen to those permissions if the file is moved to another folder? The rules in Windows 2000 regarding copying and moving files are the same as they were in Windows NT 4.0 and by default, a file will keep the permissions that are assigned to it when moving the file to another folder on the same NTFS partition. If the file is moved to another NTFS partition the file will inherit the permissions of the destination folder or partition. If a file is copied to any location, it will inherit the permissions of the destination folder or partition.

4.4.5 Shared Resources Management

Windows 2000 is designed to provide extensive network services; the security of resources via the network must be a high priority. The normal users of the system are not granted the permission to create shares on their local machines. Only Administrators and Power Users have this right to do so.

Three permissions are available for a shared folder, which may be applied to a user or a group; (1) Full Control, (2) Change, and (3) Read. These permissions are independent of the permissions set using NTFS security options. Windows 2000 uses both NTFS permissions and Share level permissions to decide the access a user will have to an object. When there are conflicting levels of permission for an object. Windows will determine the least restrictive permission both for the NTFS security and the share security. It will then compare those two permissions and the more restrictive of the two will be the resultant permission for the user. The exception to this rule is if a user has been given the Deny - Full Control permission, this takes precedence over the other permissions.

4.4.6 The NULL Session

For a system to provide shared resources it must communicate with the network and this communication is done via anonymous connections from system to system. If the system is not connected to Internet, this may not present a problem, but if the machine is directly connected lo the Internet, this operation may allow an attacker to learn about the inside network without authorisation.

This is called a NULL session connection, and is when an attacker connects as the anonymous logon. User should disable the NULL session and this can be done via any of the Security Templates. The steps for this are as follows: (1) Open any one of the security templates in the MMC, (2) Navigate to Local Policies, (3) Navigate to Security Options, and (4) Set the Additional Restrictions for Anonymous Connections to No Access Without Explicit Anonymous Permissions'.

4.4.7 Registry Management

The Windows 2000 Registry stores the configuration data for the computer, and as such is obviously a critical item to secure properly. The Registry in Windows 2000 can be directly updated with the tools like Regedit.exe and Regedt32.exe. As mentioned earlier it is recommended that Regedt32.exe be used as permissions can be applied to individual keys as you see fit. When setting the primary permissions in the Registry, however, you only have Read and Full Control to choose from.

The following lists are the permissions that are available for Registry:

- Query Value - Ask for and receive the value of a Key

- Set Value - Change a Key Value
- Create Subkey - Create a Subkey
- Enumerate Subkey - List the Subkey
- Notify - Set Auditing
- Create Link - Link this Key to some other Key
- Write DAC - Change Permissions
- Read Control - Find the Owner of a Key
- Write Owner - Change Ownership of a Key
- Delete - Delete the Key.

The permission "Full Control" is equivalent to all permissions listed above and the "Read" permission is equivalent to the Query Value.

4.4.8 Default Registry Configurations

There are systems in place to protect the Registry by default. Administrator SYSTEM account should have Full Control to all areas of the Registry. Power users are given permission to create subkeys in the HKEY__LOCAL_ MACHINE\SOFTWARE\ key, which allows them to install new software packages. Power users then have Full Control over the subkeys they create, as does the CREATOR OWNER Account. The extent of control for power users does not expand into all areas of the Registry. For example, in the Hardware hive of the Registry power users are not on the list to set permissions, by default. While making changes to areas of the Registry, be sure to have planned out the changes very carefully, as unintended actions can happen very easily and quickly.

Steps for Configuring Registry Permissions are given below:

a. Logon as Administrator.

b. Open Regedt32

c. Select HKEY_LOCAL_MACHINE

d. Expand SAM and leave the Greyed out SAM selected, choose Security from drop-down option and select permissions.

e. In this give Administration Full Control permission.

f. Expand SAM and notice that user and account information is now visible.

4.4.9 Registry Backup Management

To Secure the Registry, a backup strategy for the organization should be implemented.

There are several methods in which to backup the Registry; the first of these is to go through the Registry itself to save Subkeys/files, use the Microsoft Backup program. The Microsoft Backup utility can create a full backup of the System State, which includes the Registry configuration information. The storage option for backups is critical and a compromised system state backup is dangerous. The main files to secure, in regards to Registry Backup, is in the Operating System files, and stored in the % system root%\repair folder are the settings that must be secured. This folder contains the Registry configuration information that is needed in the event the system needs to be repaired.

Steps for saving the Registry information are given below:

a. Open Regedt32 and select software subkey of HKEY_LOCAL_MACHINE.

b. From drop-down option select Save Key.

c. Create a folder Reg_keys_folder in NTFS partition and create soft_1 as the file name and press save and close the Registry Editor.

d. Again go to Reg_keys_folder, right click and select security tab. Configure the security such that only user3 has Full Control, and remove any access to any other user account or group.

4.4.10 Printer Security Management

Printer Security in Windows 2000 provides three permissions: Print, Manage Printers, and Manage Documents. The Print option is the default level of security provided to users. This means they are provided the right to print, pause, resume, restart, and cancel documents they have submitted to a printer. To provide more control to a user, you can give them the permission of Manage Documents. With this level of permission, they are able to get the right to pause, resume, restart, and cancel all documents that have been submitted to this printer. You can also give Manage Printer permission and this level of permissions means they are given the right to share the printer, change printer permissions, change printer properties, and delete printers.

More control still over the printer can be acquired through advanced setting of printers. In the advanced settings of a printer, you can define the hours in which the printer is available. If the printer is to be used during only business hours, there is no reason to have the hours of the printer state it may be used 24x7. This type of control helps to keep the device used for official purposes only. You should secure the spooler that holds print jobs waiting to print and if the spooler is left at the default, it is in the % system root %, allows Everyone Full Control. This location should be moved to a secure NTKS location and should be managed individually.

☞ Check Your Progress 2

1) a. Create three domain user accounts: trainee1, trainee2, trainee3

   b. Limit trainee1 so that this account can log on to the network during 10 AM to 5 PM during week days (i.e., Monday to Friday).

   c. Set expiry date for trainee3 from 3 days from the today's date.

2) Describe policy inheritance.

   .....

   .....

   .....

3) Create security template with following parameters.

   - Password History 30 passwords
   - Maximum Password age of 15 days and Minimum password age of 3 days.
   - Minimum password length 12 characters.
   - Account Lockout duration 0 minutes
   - Account Lockout Threshold of 4 invalid Logon attempts.
   - Reset Account Lockout Counter after 70 minutes

4.5 WINDOWS 2000 NETWORK- SECURITY AND MANAGEMENT

4.5.1 NAT and ICS

In the previous section all of the security systems and methods are for securing operating system and data on physical hard disk. This security system is of no use if an attacker is able to sniff network packets.

Network Address Translation (NAT), is used to mask internal IP addresses with the IP address of the external Internet connection. Networks require NAT in their security policies to add an additional security "layer" between the Internet and the intranet. NAT functions by taking a request from an internal client and making that request to the Internet on behalf of the internal client. In this configuration clients on the internal network, on local LAN, are not required to have a public IP address, thus conserving public IP addresses. The internal clients can be provided with an IP address from the private network blocks. Private IP addresses are not routed on the Internet and the address ranges are:

Private IP Addresses

10.0.0.0- 10.255.255.255

172.16.0.0- 172.31.255.255

192.168.0.0-192.168.255.255

However, Microsoft has designated a range for private addressing, 169.254.0.0 - 169.254.255.255.

NAT is an integral part of Routing and Remote Access Services (RRAS), as well as part of Internet Connection Sharing (ICS). The version of NAT used by ICS is scaled down form the full version, and does not allow for the level of configuration that the RRAS NAT allows. ICS is for a small office or for a home network, where there is one Internet connection that is to be shared by the entire network. All users connect via a single interface, usually connected via a modern, DSL, or cable access point.

4.5.2 RRAS, RADIUS, and IAS

The Windows 2000 RRAS is made of several components, including: (1) Network Address Translation (NAT), (2) Routing protocols (RIP, OSPF), (3) VPN support (L2TP and PPTP), and (4) Demote Authentication Dial-In Service (RADIUS).

The Remote Access Server of RRAS allows for PPP connections and accomplish required authentication. For authentication, RRAS can use the Remote Authentication Dial-In User Service (RADIUS), or Windows Authentication. If RRAS is using RADIUS, when a user request for authentication is made to the RRAS server, the dial-in credentials are passed to the RADIUS server. The RADIUS server then performs the authentication and authorisation to access for the client to access the network.

The Remote Access Policy is controlled via the Internet Access Server (IAS), which is the Microsoft version of RADIUS. The RRAS server itself does not control the Remote Access Policy. The IAS performs several functions for remote users of the network, including authentication, authorization, auditing, and accounting to those users who connect to the network via dial-up and VPN connections. For authentication, IAS allows for great flexibility, accepting PAP, CHAP, MS-CHAP, and EAR EAP is Extensible Authentication Protocol, and is used in conjunction with technologies such as: Smart Cards, Token Cards, and One-time passwords.

4.5.3 IPSec

IPSec is a framework for ensuring secure private communications over IP networks. IPSec provides security for transmission of critical and sensitive information over unprotected networks such as the Internet. Ipsec VPNs use the services defined within Ipsec to ensure confidentiality, Integrity, and authenticity of data communications over the public network, like Internet. IPSec operates at the network layer, protecting and authenticating IP packets between participating IPSec devices. The IPSec provides the following network security services.

- Data Confidentiality – The IPSec sender can encrypt packets before transmitting them across a network.
- Data Integrity – The receiver can authenticate packets sent by the IPSec sender to ensure that the data has not been altered during transmission.
- Data Origin Authentication – The IPSec receiver can authenticate the source of the IPSec packets sent. This service is dependent upon the data integrity service.
- Anti-Replay – The IPSec receiver can detect and reject replayed packet.

In Windows 2000, you have two options for IPSec implementation, Transport Mode, and L2TP Tunnel Mode. Transport mode is designed for securing communication, between nodes on an internal network. L2TP Tunnel Mode is designed for securing communications between two networks.

IPSec Features

Two high level features of IPSec are the Authentication Header (AH) and the Encapsulated Security Payload (ESP). The AH is used to provide data communication with both integrity checking and source authentication and ESP is used to provide confidentiality. When using IPSec to secure communication, both the sender and the receiver (and only those two) know the security key used. Once authenticated, the receiver knows that the communication in-fact comes from the sender, and that the data has not been modified.

Since IPSec is works at the IP layer, it is able to secure communications with multiple protocols, including TCP, UDP, and ICMP. From a user viewpoint, the implementation of IPSec is transparent; the user is not required to modify user's environment in any way to use IPSec.

Windows 2000 IPSec Components

The Windows 2000 implementation of IPSec uses three components; (1) IPSec Policy Agent Service, (2) Internet Key Exchange (IKE), and Security Associations (SA). The IPSec Policy Agent Service gets the IPSec policy as configured in Active Directory, or the Registry, and provides that information to the IKE. Every Windows 2000 machine runs the IPSec Policy Agent Service, and the policy is pulled when the system starts as Active Directory settings are applied.

The IKE manages Security Associations (SA) and creates and manages the actual authentication keys that are used to secure the communications. This happens in two distinct steps; (1) in the first step is the establishment of a secure authenticated channel of communication, and (2) the second step the Security Associations are determined. The as are used to specify both the security protocol and the key that will be implemented.

IPSec Implementation Options

The configuration may be applied in Active Directory or directly to the Registry. IPSec policies may be applied to to computers, domains, OUs, or other GPOs in the Active

Directory. The IPSec options are in Group Policy, under Security Settings.

There exist three policy options that are predefined for IPSec implementations. They are: Client (Respond Only), Server (Request Security), and Server (Require Security).

- **Client (Respond only)** – As per this policy the secure communications are not secured most of the time. Computers with this policy respond to a request for secure communication by using a default response. If a client needs to access a secured server, it can use normal communications.
- **Server (Request Security)** - Communication must be secured most of the time, and will allow unsecured communications from non IPSec-computers. It will request IPSec from the client first, and open a secured communication channel is the client can respond securely.
- **Server (Require Security)** - This policy states that communication must always be secured and all traffic must use IPSec or it will not be accepted, and the connection will be dropped.

4.6 ENCRYPTING FILE SYSTEM MANAGEMENT

In this section we will discuss about the encryption of file system.

4.6.1 Encrypting File System (EFS)

The main benefits of personal computers are that it provides you the flexibility to boot into multiple Operating Systems for desired use. But this flexibility poses great difficulty in the world of security. In addition to the security risks of multiple Operating Systems, there are security risks introduced with the use of laptop computers. Laptops often get stolen or misplaced, and the data on that computer is vulnerable to compromise as soon as the location of the laptop is changed. With NTFS security you are able to solve the issues of security to a certain extent. As detailed there are tools available to access data even properly secured on an NTFS partition.

The concept of encryption has been introduced to solve this problem. Data encryption works to make the files on the computer only useful to the authorised owner of the data. Some of these methods provide a password for each encrypted file, which while effective, is not practical for large volumes of files. Another method is to use a key to unlock each file that has been encrypted, with only one user holding the key and Microsoft's EFS uses this approach. EFS use "public key cryptography" for encryption/ decryption of data. Public key cryptography is the use of two keys, one performs encryption and another performs decryption. The keys are keys are mathematically related. The files are encrypted by DES encryption algorithm in EFS. EFS supports file encryption for both on a local hard drive and on a remote file server. But, any files encrypted on the remote server will be transmitted over the network in clear-text by default. So, the file is decrypted at the file server, and then sent to the user. In order to maintain the high level of security, a mechanism should be implemented to secure the network traffic, such as IPSec.

The implementation of EFS works directly with NTFS and data can only be encrypted on an NTFS partition. EFS can encrypt any temp files created along with the original, and the keys are stored in the kernel using non-paged memory, so they are never vulnerable to attackers.

4.6.2 EFS and Users Management

One of good or bad point of EFS is that its use does not require any administrative effort and keys are created automatically, if the user does not already have a public key

pair to use. Files and Folders are encrypted on a single file or single folder basis, each with a unique encryption key and as they are encrypted uniquely, if you move an encrypted file to an unencrypted folder on the same partition, the file will remain encrypted. If you copy an encrypted file to a location that allows for encryption, the file will remain encrypted.

The EFS is a very transparent in use and user may have encryption enabled without aware of it.

4.6.3 Data Recovery Management

EFS designed to be implemented by a user, and is designed to be transparent; it can be used where it was not initially intended. EFS allow for Recovery Agents and the default Recovery Agent is the Administrator. These agents have configured public keys that are used to enable file recovery process. But, the system is designed in such a way that only the file recovery is possible and the recovery agent cannot learn about the user's private key.

Data Recovery for those companies and organisations that have the requirement of accessing data if an employee leaves, or the encryption key is lost.

The policy for implementing Data Recovery is defined at a Domain Controller. And this policy will be enforced on every computer in that domain. In case EFS is implemented on a machine that is not part of a domain, the system, will automatically generate and save Recovery Keys.

4.6.4 EFS Cryptography Management

As mentioned in the previous sections EFS uses public key cryptography, based on the DES encryption algorithm. Data is encrypted by what is called a File Encryption Key (FEK), which is randomly generated key. The FEK itself is then encrypted using a public key, which creates a list of encrypted FEKs. The list is then stored with the encrypted file in a special attribute called the Data Decryption Field (DDF). When a user needs to decrypt the file, he or she will use the private key that was part of the key pair. User performs encryption from the command line, or from Explorer. In Explorer, the option to encrypt is under the advanced option on the properties Window. When using the command line version, the command is, cipher, with a/e switch for encryption and a/d switch for decryption.

☞ Check Your Progress 3

1) Expand the following:

   a. RADIUS

   b. NAT

   c. ICS

   d. RRAS

2) What do you understand by VPN? Discuss IPSec security.

   .....

   .....

   .....

3) Discuss in detail EFS (Encrypting File System)]

.....

.....

.....

4) What do you understand by a null session? How null session can be disabled?

.....

.....

.....

4.7 SUMMARY

This unit covers in detail the various security and management issues that can be implemented in windows 2000 architecture. The unit address broad sweep of security and management related issues: User Authentication Management- users and group management; resource management; windows network management ; and encrypting file system management. Windows 2000 authentication covers the Subsystems components, and kerberos.

The users and group security in unit covers the topics like; configuring users accounts, windows 2000 groups (default group types, local groups, global groups, group policies etc), security configuration tools, and configuration and analysis tools. In unit covered the resource management in detail and it covers the areas like; files and folder management, files/folder permissions, inheritance and propagation, moving data and permissions, shared resources, null session, printer management, and Registry management.

The network management has been covered in detail in this unit and various network security methods like NAT, ICS, RRAS, RAS, IAS, and IPSec are covered. The unit also talks about the EFS (Encrypting File System) management of Windows 2000 systems and it covers topics like data recovery and EFS cryptography. This unit introduced the management of configuration required to secure Microsoft Windows Computer Systems and now you will be able to examine everything from the foundation principles of Windows 2000 security and management, upto to the advanced issues of securing windows 2000 running Active Directories.

4.8 SOLUTIONS/ ANSWERS

Check Your Progress 1

1) (a) False , (b) False, (c) True (d) False.

2) Windows 2000 can use the following for authentication: Kerberos, NTLM, RADIUS, SSL, Smart Cards, and more.

3) When a user the log on process by entering his credentials, Windows will contact an Active Directory domain controller, and locate the Kerberos Key Distribution Center (KDC). An Authentication Server (AS) performs the actual authentication. The KDC responds by issuing a Ticket Granting Ticket (TGT) to the authenticated user. The TGT contains identification information about this user to various servers on the network, and is used to gain further access in the network. After the user account has been authenticated, the TGT is used to

request further Kerberos tickets in order to access network services. The machine that provides the tickets for the network resources to the authenticated client is known as a Ticket Granting Server (TGS).

Check Your Progress 2

1) a. Open the management console MMC.

   b. Open or add the Active Directory Users and Computer Snap-In.

   c. Expand domain listing, to view the console tree.

   d. In the Action down menu, select option New User.

   e. Create new users, trainee1, trainee2, trainee3, etc.

b) i. Open the Active Directory Users and MMC Snap-in

   j. Expand domain listing, to view console tree.

   k. Select user folder.

   l. Double click trainee1.

   m. In the Property Window, choose Account Tab, and select the Logon Hours Option.

   n. Limit trainee1 so that this account can log on to the network during 10 AM to 5 PM during week days (i.e Monday to Friday).

   o. Press OK to close the Logon Hours dialog box.

   p. Again press OK to close the trainee1 Property Window,

c) g. Open Active Directory Users and Computers MMC Snap-In.

   h. Expand domain listing to view the console tree.

   i. Select user folder.

   j. Double click trainee3 and in property window select the Account tab.

   k. In the Account Expires Option, and select End of option, and enter desired expiry date.

   l. Press OK.

2) Policy Inheritance is the name for the process of a user or computer inheriting the final policy configuration from multiple policies, depending on where the object may be in the Active Directory hierarchy and configured GPOs.

3) • Open MMC and select Add/Remove Snap-Ins.

   • Click on Add button, and add Security Templates Snap-In.

   • View all templates by expanding Security Templates.

   • Right Click Directory Location(e.g. :\Winnt\Security\Templates. and press New Template.

   • Enter template name: Custom Template

   • Enter Description: Template for highly secure passwords.

   • Press OK

   • Apply following configuration settings to Custom Template:

   • Password History 30 passwords

- Maximum Password age of 15 days and Minimum password age of 3 days.
- Minimum password length 12 characters.
- Account Lockout duration 0 minutes
- Account Lockout Threshold of 4 invalid Logon attempts.
- Reset Account Lockout Counter after 70 minutes.
- Right Click and press Save.

Check Your Progress 3

1) RADIUS – Remote Authentication Dial in Service, (b) NAT- Network Address Translation, (c) ICS- Internet Connection Sharing, (d) RRAS- Routing and Remote Access Services.

2) Virtual Private Network. IPSec is a framework of pen standards for ensuring secure private communications over IP networks. IPSec provides security for transmission of critical and sensitive information over unprotected networks such as the Internet.

3) EFS works directly with NTFS and data can only be encrypted on an NTFS partition. EFS can encrypt any temp files created along with the original, and the keys are stored in the kernel using non-paged memory, so they are never vulnerable to attackers.

4) For a system to provide shared resources it must communicate with the network and this communication is done via anonymous connections from system to system. If the system is not connected to Internet, this may not present a problem, but if the machine is directly connected lo the Internet, this operation may allow an attacker to learn about the inside network without authorization. This is called a NULL session connection, and is when an attacker connects as the anonymous logon.

Disabling null session:

c) Open any one of the security templates in the MMC,

d) Navigate to Local Policies,

e) Navigate to Security Options, and

f) Set the Additional Restrictions for Anonymous Connections to No Access Without Explicit Anonymous Permissions'.

4.9 FURTHER READINGS

1) Windows 2000 Professional Resource Kit, Microsoft Press.

2) *Cryptography and Network Security, Principles and Practice,* SE, PE., William Stallings

3) *Security in Computer,* Charles P. P fleeger and Shari Lawrence Pfleeger, Third Edition, Pearson Education.

4) *Windows 2000 Commands* by Aleen Frisch.

5) Microsoft Web Site http://www.microsoft.com.