Department of Energy

CIAC

Computer Incident Advisory Capability

Windows NT Network Security A Manager's Guide

CIAC-2317

Marcey Kelley
Lawrence Livermore National Laboratory

Wendall Mayson
Westinghouse Savannah River Company

December 1997

UCRL-MA-128827

CIAC is the U.S. Department of Energy's Computer Incident Advisory Capability. Established in 1989, shortly after the Internet Worm, CIAC provides various computer security services to employees and contractors of the DOE, such as:

- Incident Handling Consulting
- Computer Security Information
- On-site Workshops
- White-hat Audits

CIAC is located at Lawrence Livermore National Laboratory and is a part of its Computer Security Technology Center. CIAC is also a founding member of FIRST, the Forum of Incident Response and Security Teams, a global organization established to foster cooperation and coordination among computer security teams worldwide.

Reference to any specific commercial product does not necessarily constitute or imply its endorsement, recommendation or favoring by CIAC, the University of California, the United States Department of Energy, or the United States Government.

This is an informal report intended primarily for internal or limited external distribution. The opinions and conclusions stated are those of the author and may or may not be those of the Laboratory. Work performed under the auspices of the U. S. Department of Energy by Lawrence Livermore National Laboratory under Contract W-7405-Eng-48.

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information
P.O. Box 62, Oak Ridge, TN 37831
Prices available from (423) 576-8401, FTS 626-8401.

Available to the public from the
National Technical Information Service
U.S. Department of Commerce
5285 Port Royal Rd.
Springfield, VA 22161

Table of Contents

Part I: NT Security Mechanisms

Many DOE sites have been upsizing from Windows 3.11 or Windows 95 to the Windows NT operating system. In today's environment, it is important to migrate to Windows NT because it was built from its inception to incorporation networking, security and audit reporting as services within the operating system.

What is the basis for NT security? It is designed to help enforce an organization's security policy (See Appendix A for details on Security Policies). This policy specifies an organization's information protection requirements, access controls, and audit requirements. NT enables you to configure your network to allow information to be separated by departments or users in need-to-know groups and to control access by "outsiders". It further enables you to manage network and organizational resources as a group of objects and to enforce security rules controlling access and authentication.

Since NT is built to be secure, you don't have to worry about someone breaking into your system, right? Wrong. NT provides the ability to have a highly secure system only with the correct configuration and object access controls. Operating systems don't make security problems go away. There is not an operating system available today that can provide you with a complete security solution.

Remember you must define a security plan that defines the level of security needed in your organization, and integrate Windows NT with its security features into that plan. Security plans must detail both physical and logical security measures, to build the best protection against intrusion on your systems.

NT Terminology

Described in this section are the basic concepts in the Windows NT environment. The concept of objects is important to the overall security theme in this operating system. The difference between the two types of NT software is defined, as well as the difference between domains and workgroups. Additional terminology included in this section is concepts regarding the NT Registry and C2 Security.

Objects in NT

Described in this section are the basic concepts in the Windows NT environment. The concept of objects is important to the overall security theme in this operating system. The difference between the different types of NT software is defined, as well as the difference between domains and workgroups. Other terminology included in this section is concepts regarding the NT Registry and C2 Security.

Most elements in the NT operating system are represented as objects. Objects can be files, directories, memory, devices, system processes, threads, or desktop windows. Objects are what provide the NT operating system with a high level of security. They hide data from the outside and provide information only as defined by the object's functions. This gives a

layer of protection against external processes accessing internal data directly. NT obtains its high security level by preventing programs direct access to objects. All actions on objects must be authorized and performed by the operating system.

Objects can be secured in NT by setting attributes described by a security descriptor, or access token, containing the following:

- Owner/User Security ID (SID) indicating who owns the object.
- Group SID only used by the POSIX subsystem.
- Discretionary access control list contains access permissions for users and groups, controlled by the owner of the object.
- System Access Control List (ACL) controls the creation of auditing messages.

There are two types of objects: container objects and non-container objects. Container objects hold other objects; non-container objects do not have the ability to include other objects. Directories are container objects and files are non-container objects. Child objects created within a parent container inherit permissions from the parent object.

NT Server vs. NT Workstation

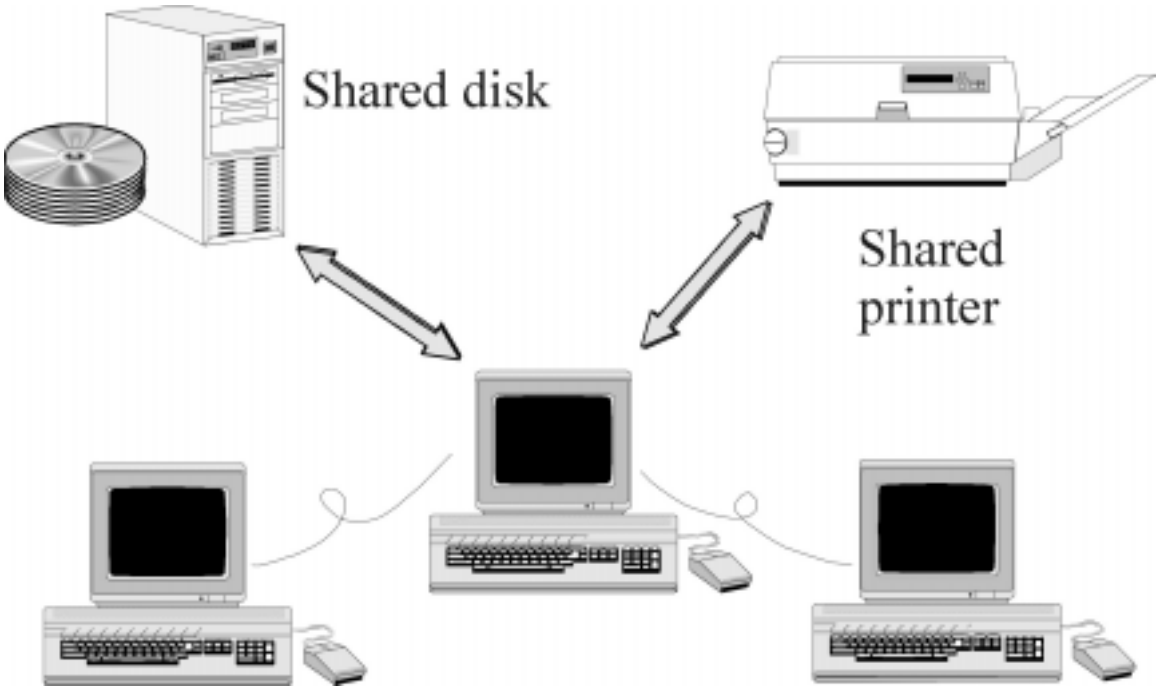
There are two different types of Windows NT software available: Windows NT Workstation and Windows NT Server. The Server version is the same as the Workstation version except that it provides additional features for networking. Only ten users can access a Windows NT Workstation at a time, and NT Server can be accessed by an unlimited number of users dependent upon the license purchased.

There may be some confusion between a server and a Windows NT Server. Windows NT Server is a piece of software, where a server is a piece of hardware.

Workgroups

There are two types of networking configurations in Windows NT: Workgroups and Domains.

A workgroup is an organizational unit of a single system, or multiple systems not belonging to a domain. Systems in a workgroup individually manage their own user and group account information and their own security and account policy databases. They do not share this information with any other systems. If a system is not part of a domain, it is automatically part of a workgroup. The best use of the workgroup configuration is for small groups of systems with few users, or where the network is configured without an NT Server.



• Figure 1: Workgroup Model Illustration

Warning	Security for Workgroups with systems running Windows 95, Windows 3.x, or Windows for Workgroups is virtually eliminated due to the fact that anyone can access the computers and copy files to a diskette. There is no secure logon process or object access controls to prevent users from accessing sensitive files. Therefore, the workgroup model is not recommended unless the systems are all running Windows NT.

Domains

A domain is a collection of servers that are grouped together sharing a security policy and a user account database. Centralizing the user account database and security policy provides the system administrator with an easy and effective way to maintain the security policies across the network.

Domains consist of a Primary Domain Controller (PDC), Backup Domain Controllers (BDC), servers and workstations. Domains can be set up to segregate different parts of your organization. Setting up proper domain configurations cannot guarantee a secure network, but it can give administrators a start in controlling user access on the network.

✔ Tip	Isolate mission critical departments and services into separate domains, and limit the number of user accounts in these domains, to have more control over users actions.

Domain Controllers

A PDC is a server in the domain that maintains the security and user account databases for that domain. Other servers in the domain can act as BDCs that hold a copy of the security database and user account information. The PDC, as well as the BDC can authenticate logon requests. The BDC provides the network with a backup in case the PDC crashes important data will not be lost. Only one PDC is permitted in each domain. The master copy of the Security Account Manager (SAM) database is

located on the PDC, where all account modifications are made. The BDCs are not permitted to make any modifications to the databases.

NT Registry

The Registry is a database that contains applications, hardware, and device driver configuration data, as well as network protocols and adapter card settings. This data is stored in the registry to provide a repository that stores and checks configuration data in one centralized location.

The functions of many files are combined in the Registry including the CONFIG.SYS, AUTOEXE.BAT, SYSTEM.INI, WIN.INI, PROTOCOL.INI, LANMAN.INI, CONTROL.INI and other .INI files. It is a fault-tolerant database that is difficult to crash. Log files provide NT with the ability to recover and fix the database if the system fails.

The Registry database structure has four subtrees:

- HKEY_LOCAL_MACHINE: Contains information about the local system including hardware and operating system data, startup control data and device drivers.
- HKEY_CLASSES_ROOT: Includes data pertaining to object linking and embedding (OLE) and file-class associations.
- HKEY_CURRENT_USERS: Contains information about users currently logged on the system, which includes the user's profile groups, environment variables, desktop settings, network connections, printers and application preferences.
- HKEY_USERS: Stores all actively loaded user profiles, including profiles of any users who have local access to the system. Remote user profiles are stored in the Registry of the remote machine.

Each of the subtrees contains value entries which are called *keys,* and each *key* can have many *subkeys.* The data in the four Registry subtrees is derived from sets of files called hives. Each hive consists of two files: data and log files. Each hive represents a group of keys, subkeys, and values that are rooted at the top of the Registry hierarchy.

C2 Security

Requirements for a C2 compliant system are defined by the National Computer Security Center (NCSC) of the United States Department of Defense, in the Trusted Computer System Evaluation Criteria document, better known as the *Orange Book*. Although a useful reference, the Orange Book only applies to stand-alone systems. NCSC security ratings range from *A* to *D*, where *A* is the highest level of security and *D* is used mostly to evaluate business software. Each range is divided into classes, and in the *C* division there are *C1* and *C2* levels of security.

C2 represents the highest level of security in its class. Windows NT 3.5 Server, as a standalone system, was designed from the ground up to comply with the NCSC's C2 level requirements, and has been successfully evaluated as such. Certain processes such as identification, authentication, and the ability to separate accounts for operator and administrator functions, have met *B2* requirements, an even higher level of security. These processes fulfill requirements for the B2 Trusted Path and B2 Trusted

Facility Management.

Windows NT Server 4.0 is currently in NCSC evaluation as the networking component of a secure system. This is defined by the *Red Book* which is NCSC's Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria, or Orange Book. The requirements are not changed in the Red Book, they just define how a networked system needs to operate in order to meet Orange Book requirements for a C2 level system.

C2 implementation on the Windows NT Server 3.5 is based solely on the software. In order to have a C2 compliant system setup, you must:

- Have no network access to the system.
- Remove or disable floppy disk drives.
- Change standard file system access to be more restrictive.

✔ Tip The C2 Config tool is available through the Windows NT Resource Kit, which can help you achieve a C2 level secure system.

The most important C2 level requirements featured in Windows NT 3.5 are:

- Discretionary access control (DAC): allows an administrator or user to define access to the objects they own.
- Object reuse: Memory is protected to prevent read access after it is freed from a process. When objects are deleted, users will be denied access to the object even when that object's disk space has been reallocated.
- Identification and authentication: Users must uniquely identify themselves before any access to the system is obtained. This is accomplished by entering a unique name, password, and domain combination, which will produce a users unique identity.
- Auditing: Must be able to create, maintain, and protect against modifications of an audit trail of access to objects. Access to the audit information must be restricted to a designated administrator.

NT Security Model

The Windows NT security model affects the entire Windows NT operating system. It provides a central location through which all access to objects is verified so that no application or user gets access without the correct authorization.

NT Security Subsystem

The Windows NT security model is based on the following components:

- Local Security Authority (LSA)

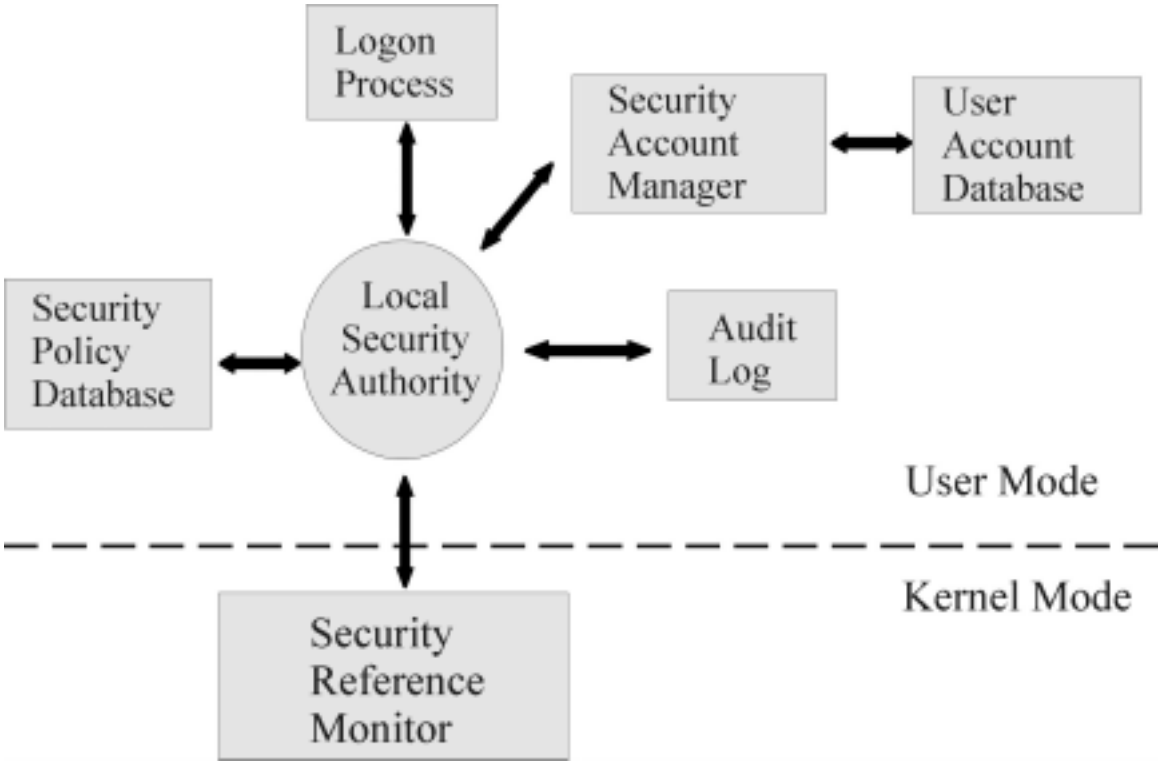
- Security Account Manager (SAM)
- Security Reference Monitor (SRM)

In addition to these components, NT also includes logon processing, access control and object security services. Together these elements form the foundation of security in the Windows NT operating system, which is called the security subsystem. This subsystem is known as an integral subsystem since it affects the entire operating system.

Local Security Authority (LSA)

The LSA is the heart of the security subsystem. It has the responsibility of validating local and remote logons to all types of accounts. It accomplishes this by verifying the logon information from the SAM database. It also provides the following services:

- Checks user access permissions to the system
- Generates access tokens during the logon process
- Manages local security policies
- Provides user validation and authentication
- Controls the auditing policy
- Logs audit messages generated by the SRM



- Figure 2: NT Security Model

Security Account Manager (SAM)

The SAM manages a database which contains all user and group account information. SAM provides user validation services which are used by the LSA, and are transparent to the user. SAM is responsible for checking logon input against the SAM database and returning a secure identifier (SID) for the user, as well as a SID for each group to which the user belongs. When a user logs on, the LSA creates an access token which includes the SID information along with the user's name and associated groups.

From this point on, every process that runs under this user's account will have a copy of the access token. When a user requests access to an object, a comparison is made between the SID from the access token and the object's access permissions list to validate that the user has the correct permissions to access the object.

The SAM database supports a maximum of 10,000 accounts. SAM databases may exist on one or more NT systems, depending on the network configuration. The types of network configurations include:

- When separate user accounts are on each system, the local SAM database is accessed.

- The SAM database is located on the domain controller when a single

domain with a centralized source of user accounts is the configuration.

- In the master domain configuration, where user accounts are also centralized, the SAM database is located on the Primary Domain Controller (PDC), which is copied to all Backup Domain Controllers (BDC) in the master domain.

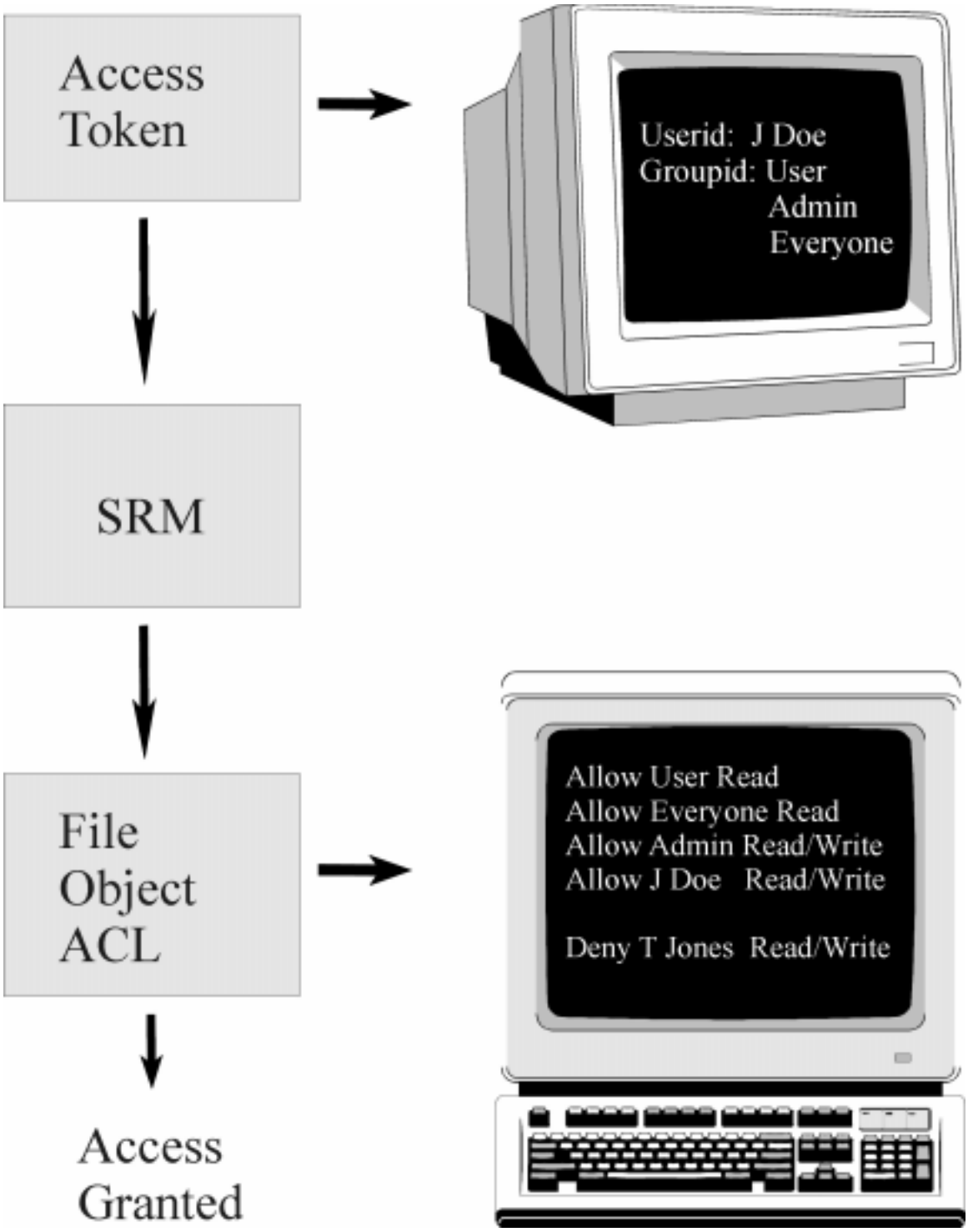
Security Reference Monitor (SRM)

The SRM runs in kernel mode and is a component of the Windows NT Executive. It is responsible for the enforcement of access validation and audit generation policies required by the LSA. SRM provides services for access validation to objects and access privileges to user accounts. It also protects objects from being accessed by unauthorized users. To ensure that objects are protected regardless of their type, the SRM maintains only one copy of the access validation code on the system. Instead of accessing objects directly, users requesting access to objects must have SRM validation. The steps used to determine user access to objects are as follows:

When access to an object is requested, a comparison is made between the file's security descriptor and the SID information stored in the user's access token. The user will obtain access to the object given sufficient rights. The security descriptor is made up of all the Access Control Entries (ACE) included in the object's Access Control List (ACL).

When the object has an ACL, the SRM checks each ACE in the ACL to determine if access to the object is granted. If the object has no ACL associated with it, SRM automatically allows access to everyone. If the object has an ACL with no ACEs, all access requests to that object will be denied.

After the SRM grants access to the object, continued validation checks are not needed to access the particular object. Any future access to the object is obtained by the use of a handle which was created when the access was initially validated.



- Figure 3: SRM Access Validation Process

NT Logon Windows NT logon processes provide mandatory logon for user identification and cannot be disabled. Before accessing any resources on the system, the users go through the logon process so that the security subsystem can authenticate the user name and password.

To protect against an application running in background mode, such as a Trojan logon program, the logon process begins with a *Welcome* message box that requests the user to press Ctrl, Alt and Del keys before activating the actual logon screen.

Note The Ctrl, Alt, Del sequence guarantees that a valid Windows NT logon sequence will be initiated. This key sequence should always be used when logging on to a machine, even if it appears that the logon screen is already displayed.

Logon Banner

A logon banner, also referred to as a warning banner, should be added to warn individuals who may try gaining access to a system without authorization. If activated, this message is displayed after the *Welcome* message in a dialog box that must be confirmed. The text and style of the legal notice is set in the Registry Editor. (See Appendix B for examples).

Warning Security policies must specify the use of legal notices. These notices can be posted on bulletin boards throughout an organization and on logon screens of users systems. If legal notices do not exist, users may take the liberty of browsing the network and access directories and files without restrictions.

DOE orders specifically warn against the misuse of government property. The Department of Justice further warns that logon banners are required anytime you are monitoring computer users for unauthorized access. Without them, prosecution of computer abuse cases is very difficult. Examples of logon banners for DOE and the Department of Justice are described in Appendix D.

NT Logon Process

Outlined in Figure 4 is the Windows NT logon process:

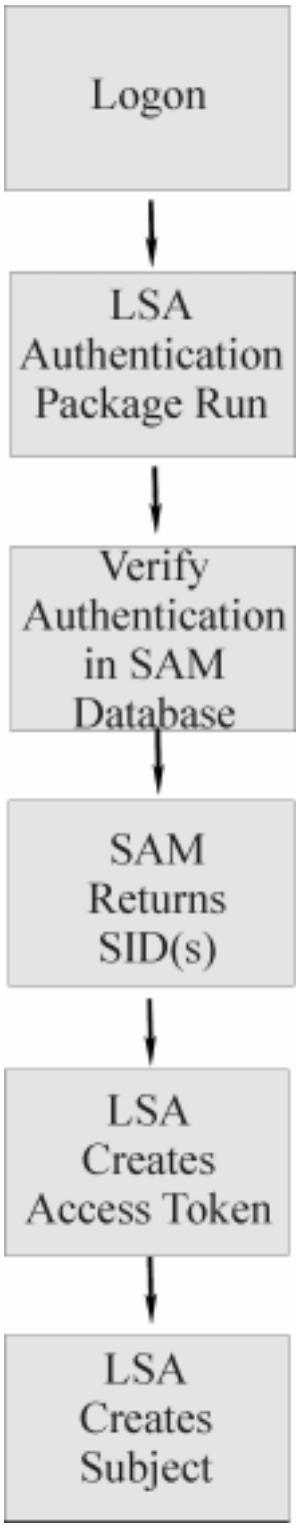
A *Welcome* dialog is displayed which requires a user name, password and the server/domain the user would like to access. If the user information is valid, the system proceeds to authenticate the user.

User authentication is determined by passing the user input from the *Welcome* screen to SAM via the security subsystem.

SAM does a comparison between the user logon information and the server's SAM database. If the data matches, the server notifies the workstation of the approval. The server also stores information about the user, such as account privileges, home directory location and workstation variables.

The LSA now constructs the access token. The access token is connected with each process the user runs.

This process and token information together form a *subject*. When a user requests access to an object, the contents of the subject's token are compared to the object's ACL through an access validation procedure. This access validation procedure grants or denies permission to the user's request.



- Figure 4: NT Logon Process

Part II: Designing the NT Environment

NT security components enable you to design a network configuration that separates highly sensitive data and applications from less sensitive data and applications. By designing your network according to information protection needs, you greatly simplify the application of your security policies (See Appendix C for security policy information). The NT environment uses the concept of domains as a means for grouping resources together that share common information and have common security needs. Communication between domains is then controlled by trust relationships.

For example, many areas of an organization may need access to data located within the financial domain; however, user in the financial domain probably doesn't need access to data within the medical domain. Additional ways to protect your systems are achieved by group management, access control of objects, and file system configurations, which are all discussed in this section.

Trusts and Domains

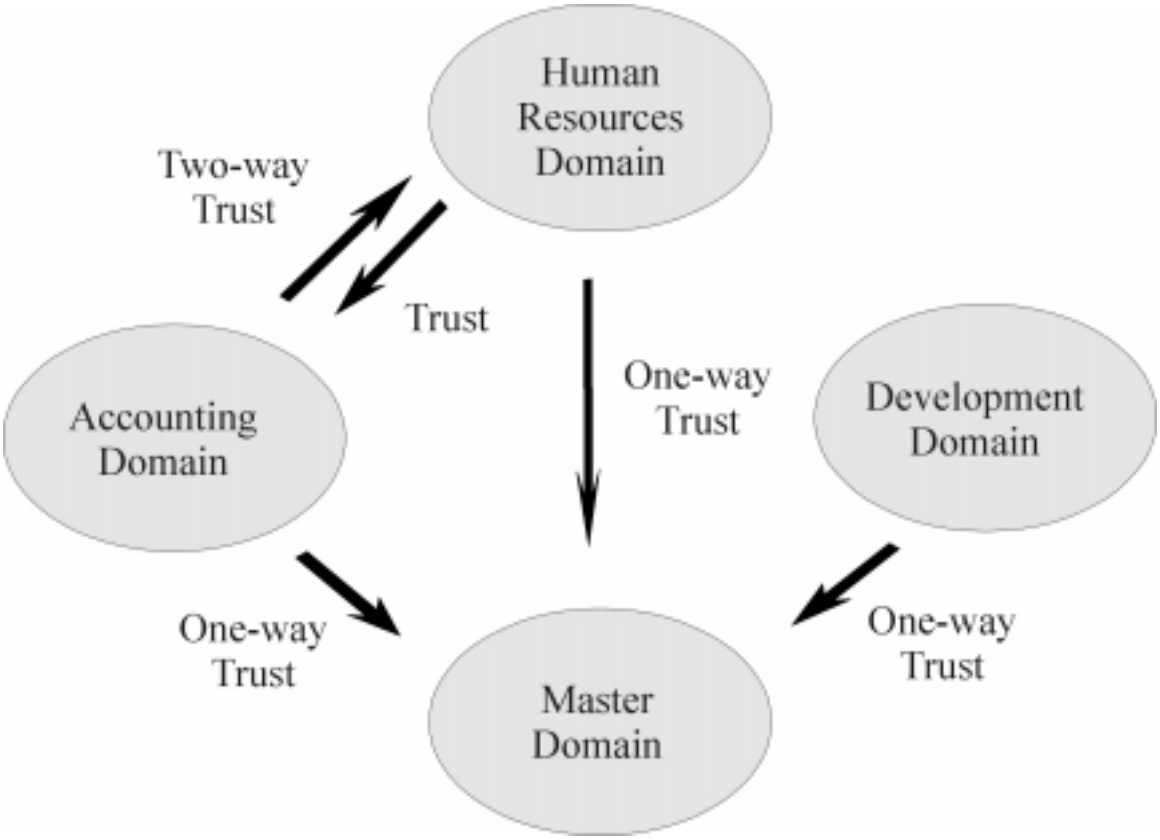
Trust Relationships

Trusts are an administrative way to link together two domains allowing one domain's users access to the other domain. Trust relationships between domains are a way to centralize administrative tasks. They enable user accounts and groups to be used in a domain outside of where those accounts originated. Trusts combine two or more domains into an administrative group. There are two parts to a trust: the trusted domain and the trusting domain. The trusted domain makes accounts available for use in the trusting domain. Users only need one name and password to access multiple domains.

✔ Tip The best policy in setting up trust relationships between domains is to provide the least amount of service possible. Evaluate the services you have running on domains. Do not allow trust relationships to a domain that might allow users to disrupt services providing critical information, and avoid running high security risk services in domains which are accessed by any users other than administrators.

Trust Relationship Models

Trust relationships are defined in only one direction. To obtain a two-way trust, both domains must trust each other. The trusted domain is where the accounts reside, known as the *account domain*. The trusting domain contains the resources, known as the *resource domain*.



- Figure 5: Trust Relationships

The following are the types of Trust Relationship Models:

- Single Domain
- Master Domain
- Multiple Master Domain

Single Domain Model

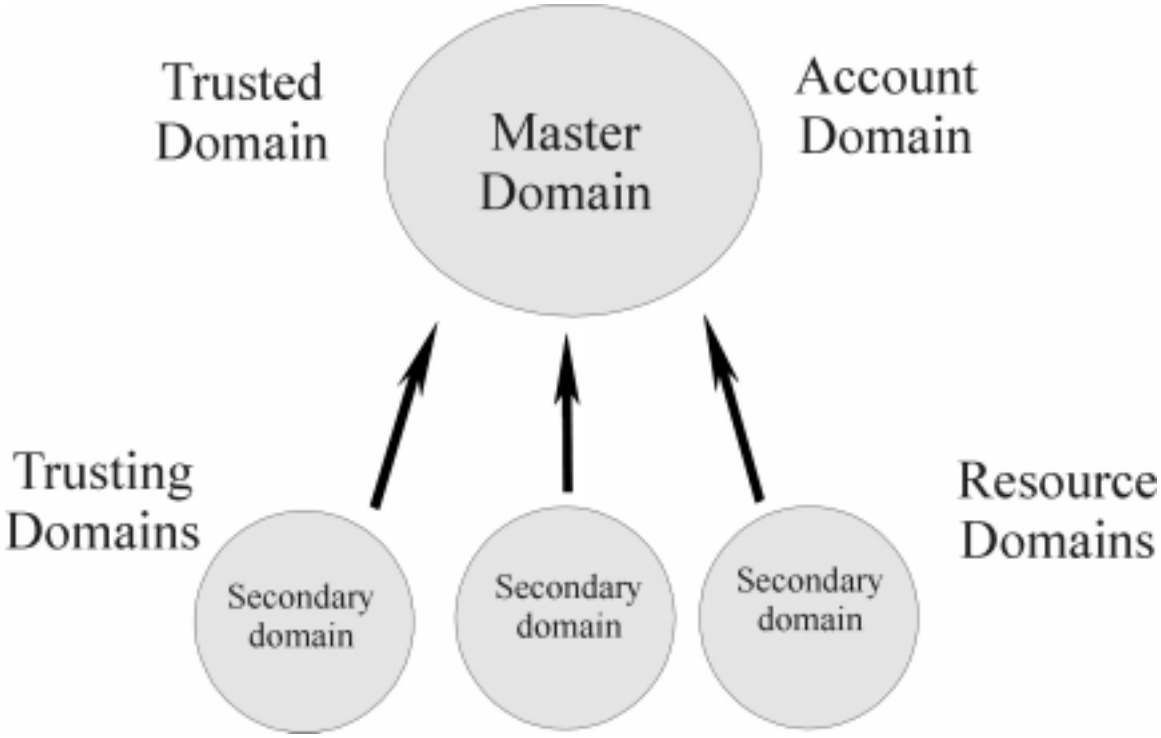
The Single Domain is the best model for organizations with fewer than 10,000 users. There is only one domain in this model; therefore there is no administration of trust relationships. Administration of user accounts is centralized, and global groups are used for accessing resources.

Master Domain Model

The Master Domain model includes multiple domains, with one being the master domain. The master domain is trusted by all other resource domains, but does not trust any of them. The resource domains do not trust each other. This model provides the benefits of centralized administration and multiple domains.

Administration of user accounts and resources are in separate domains.

Resources are managed locally on the trusting domains, while user accounts are controlled on the trusted master domain. The master domain model is used in organizations with less than 10,000 users. The number of users is limited because the accounts are all maintained on the master domain.

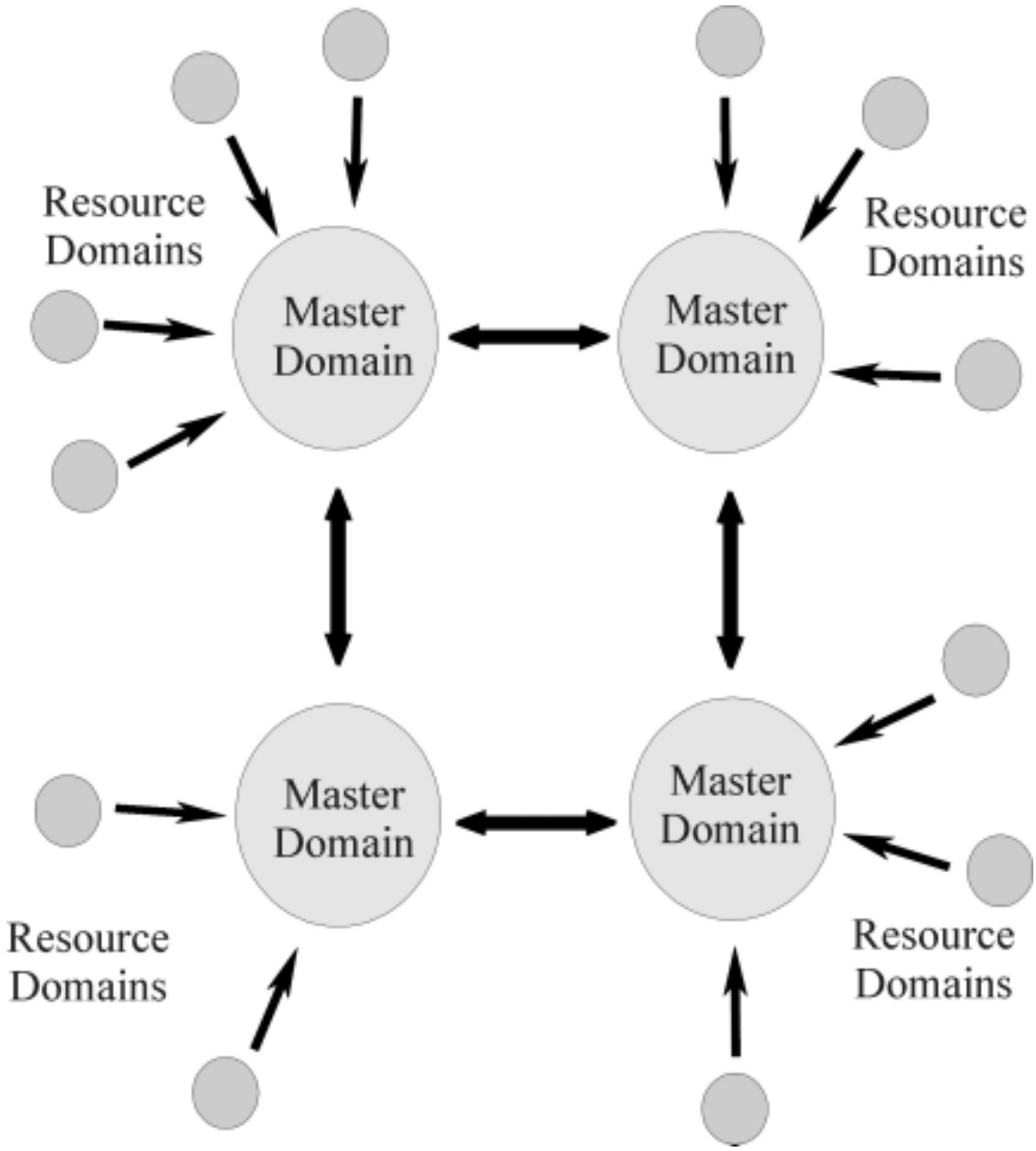


- Figure 6: Master Domain Model

Note	If done correctly, this model can provide a secure configuration because administration is managed for the entire network in one centralized location.

Multiple Master Domain Model

The Multiple Master Domain model is used for organizations with computer resources grouped into logical divisions, such as by departments or location. This model is identical to the Master Domain model except that there is more than one master domain. All master domains have a two-way trust with each other. Each resource domain trusts all master domains, but the resource domains do not trust each other. Since master domains trust each other, only one copy of the user account database is needed. This model is designed for organizations with more than 10,000 users.



- Figure 7: Multiple Master Domain Model

Group Management

Groups are an administrative tool used to provide a collection of users, with common needs, the permissions and rights they require to perform their job.

As previously mentioned, a group is essentially an account containing other accounts in Windows NT. A user in a group is a member of the group and access permissions, rights, and restrictions assigned/granted to the group

are assigned/granted to each of the group members.

For example, if a directory is established for the Payroll Department to hold their common files, it is much easier for a system administrator to have everyone in the Payroll Department in a group and then assign that group permissions on the directory and the files in it. Otherwise, the system administrator would have to go through and assign permissions to every user in the Payroll Department.

In addition, groups can be used to restrict the access a collection of users has to certain objects. For example, the system administrator could utilize the Payroll group to prevent the users in the Payroll Department from printing to a printer in a remote location (because their data could be potentially very sensitive), while allowing access for all other users, by placing a deny ACE for the Payroll group in the ACL for the printer.

It is normally easier to administer rights by granting them to groups and then making the users who need the right a member of the group. For example, if there are users who need to logon to a server locally, create a group called Local Logon. Add the users to the group, and grant the Log on Locally right to the group. This group could then be reused again should this group of users need some other common right or access permission.

There are three types of groups in Windows NT:

- Local Groups
- Global Groups
- Special Groups

Local Groups

Local groups are maintained on a local system or domain and may have user accounts or global groups as members. At the local system level, local groups would be used to administer permissions and rights for the system on which they reside. At the domain level, local groups would be used to administer permissions and rights on Windows NT Servers within the domain where the groups reside. To summarize, local groups are only utilized in the user account database for the local system or domain where they are created.

Windows NT provides some built-in local groups each with established permissions and rights. At the local system level they are:

- Administrators - can fully administer the system.
- Power Users - can share directories and printers.
- Users - normal users.
- Guests - granted guest access.
- Backup Operators - can bypass file security in order to complete backups.

At the domain level, the built-in groups are:

- All listed above except Power Users.
- Server Operators - can manage domain servers.
- Account Operators - can manage user accounts and groups.
- Print Operators - can manage printers.
- Replicator - supports file replication.

Global Groups

Global groups maintained on a Windows NT domain may have domain user accounts as members, and are used to administer domain users. System administrators can effectively use global groups to sort users based on their needs. This can be accomplished by placing the global group in the appropriate local groups, assigning the users permissions and granting them the rights they need to perform their jobs. As mentioned, global groups can only have domain user accounts as members. No other groups can be members of a global group. This is due to the fact that the system administrator assigns permissions and grant rights to the local groups (because the local system or domain server holds the resources) and then makes the global groups members of the local groups.

Windows NT provides two built-in global groups each with established permissions and rights. They are:

- Domain Admins - contains the domain administrator account by default and is a member of the domain level Administrators local group and the system level Administrators local group for Workstations in the domain.
- Domain Users - contains all the domain users.

Special Groups

Special groups are created by Windows NT for unique or specific purposes and can not be viewed, changed, or have members added to them in the User Manager. A user's membership to a special group is determined by how they access resources on the system. Special groups may be assigned access permissions in some cases and may be seen when a system administrator is assigning permissions on Windows NT objects.

The following is a list special groups and a description of their membership:

- Network - any user connected to a system via the network.
- Interactive - any user logged on interactively at a local system
- Everyone - any user logged on to the system (both the Network and Interactive groups).
- Creator Owner - the user that created or took ownership of an object.

- System - the Windows NT operating system.

Note If the user were the system administrator or other user that is a member of the Administrators group, the Administrator group would be a member of the Creator Owner group.

The special group that system administrators must pay close attention to is the Everyone group. As stated above, all users logged on are members of this group. Therefore, any access permissions assigned to the Everyone group allowing or denying access to objects is by default assigned to all users.

For example, if a file should only be accessed by a certain group, the system administrator could not assign permissions to that group allowing file access and then assign permissions to the Everyone group denying file access. Since Windows NT acts on all deny ACEs before allow ACEs, it would stop when it found the deny ACE for the Everyone group and no one would be allowed access including the group with permissions assigned to allow access to the file.

Access Control

Each file and directory object has an Access Control List (ACL) that contains a list of Access Control Entries (ACEs). ACEs provide information regarding access or auditing permissions to the object for a user or group of users. Along with the file system, they protect objects from unauthorized access.

There are three different types of ACEs:

- System Audit
- Access Allowed
- Access Denied

System Audit is a system ACE used for logging security events and audit messages. Access Allowed and Access Denied are known as discretionary ACEs. They are prioritized by the type of access: Denied and Granted. Deny always overrides grant access. If a user belongs to a group with Access Denied privileges to an object, the user will be denied access regardless of any granted access he possesses from his own user account, or in other groups to which he is included.

Discretionary ACLs allow owners to control the access of their objects. Controls over objects can be applied to individual users, multiple users, and groups. They can be set by the object's owner, a user who has an administrator account, or any user with correct permissions to control resources on the system. If a discretionary ACL is not specified for an object, a default ACL is created. Default ACL file objects inherit access controls from their parent directories.

Warning Be sure to evaluate your object's ACLs after installing Windows NT. Most versions are shipped with file ACLs set to give Everyone Full Control access.

User Rights User authorization to perform specified actions on a system is called rights. Rights apply to the entire system. They are usually assigned to groups or users by the system administrator. Rights give users access to services such as backing up files and directories, shutting down the computer, logging on interactively or changing system times, that normal discretionary access controls do not provide.

Managing NT File Systems

Due to NT's modular approach of file system management, multiple file systems are supported. NT uses low-level drivers as a part of the NT Executive to support each file system. This provides the ability to expand to additional file systems as they are introduced by simply installing a new driver.

NT 4.0 supports two file systems: NTFS and FAT.

FAT File System The File Allocation Table (FAT) file system is named after it's organizational method. The FAT file system was originally designed for small disks and simple directory structures. Its design has since evolved to support larger disks and more powerful systems. It is most widely used for systems that run the DOS operating system.

The FAT file system doesn't support the security features or the automatic disk restoration utilities that NT provides. Using the FAT file system is not recommended for volumes shared across the network. The following configurations do require the FAT file system structure:

- Dual-boot system configurations with DOS or OS/2 volumes.
- FAT is the only file system available for formatting diskettes on Windows NT.
- RISC-based systems must provide a FAT partition to boot system files. NT provides a tool to secure the FAT system partition on this type of system.

✔ Tip If there is no need to boot DOS, and the system is not an RISC architecture, using FAT file systems are not recommended.

NTFS File Systems NTFS was developed to support the Windows NT file and directory security features. It is the only file system available on NT that provides the capability to assign permissions to individual files. The NTFS driver that allows access to an NTFS volume is loaded in NT so unauthorized users cannot access NTFS volumes by booting the system from a DOS diskette.

NTFS also prevents users from undeleting files or directories that have been removed from NTFS volumes. Since NT doesn't give undeleted programs access to work on an NTFS volume, even files that still exist on the disk are not available. NTFS provides file system recovery where disk activities can

be logged to enabling activities to be restored in the case of a system crash. Chances of corrupting data, due to power or hardware failures, are small with NTFS.

Physical Security and NTFS

NTFS file system security is only valid if the ability to access the system from DOS, or another operating system is eliminated. The following precautions for physical security should be examined:

- Remove or lock floppy drives.
- Require boot passwords on servers and set the BIOS to disable booting from a floppy drive. In most cases, removing the battery disables the BIOS lock.
- Do not create any DOS partition on the server.
- Lock the system in a secure location.
- Set alarms alerting you to when a server is shut down, so an intruder can be caught during a potential attack.

Warning A program called ntfsdos.exe is available to read files protected by Windows NTFS. The program is run after booting a system with a DOS diskette. This is not a security risk if the proper physical security measures are taken or floppy drives are not available on the system.

NTFS vs. FAT

- NTFS provides extended security features not available with the FAT file system.
- NTFS is built for speed. It uses a binary tree structure for directories to reduce the access time needed to locate files.
- NTFS minimizes file fragmentation in large disk volumes.
- NTFS uses small cluster sizes (512 bytes) to prevent wasted disk space.
- NTFS provides the ability to selectively compress individual files and directories or actual volumes on disks.

Shares

The Shared Directory feature in the File Manager allows sharing of files and directories over the network. Shared object permissions can be established for FAT or NTFS file structures. The user must be a member of the Administrator group or Server Operator group to work with shared directory permissions. Users are unable to access files on a system through the network until there is a shared directory available.

Once a directory has been shared on the system, users can log on to that system and be able to access the shared directory. To use the directory, the user must assign the share to an unassigned drive letter. When the directory is assigned a drive letter, the share can be accessed just like

another hard disk on the system. Directory sharing can be viewed and stopped by an Administrator or Server Operator.

Object Permissions

File and directory permissions are the foundation of most user-controlled security in Windows NT. Permissions are the rules associated with a particular object, which describe which users can access what objects, and how they have access to the objects. Object permissions for files are only available for files stored on NTFS volumes. File and directory permissions are cumulative, but the No Access permission overrides all other permissions.

The types of file access permissions are:

- No Access
- Read
- Change
- Full Control
- Special Access

For directory access the following permissions are added:

- List
- Add
- Read

Object Ownership

Object ownership allows the user to change permissions on the owned object. The user who is the creator of a file or directory is usually the owner. Users can't give away ownership of their objects, but they can give other users permission to take ownership. This prevents users from creating objects and making them appear to be owned by another user.

Ownership of a file or directory can be taken by an Administrator without the owner's consent, but the Administrator can't transfer ownership to others. Administrators cannot access private files without leaving some trails behind, because after claiming ownership, Administrators cannot return ownership to the original owner.

Monitoring System Activities

Monitoring is a continuous evaluation of system-level attributes that could reveal system compromise. Monitoring also provides reporting and follow-up mechanisms on attempted violations to the system. Auditing systems

validates compliance when using monitoring procedures. In addition, auditing is used in follow-up actions.

There are two types of security monitoring: status and event monitoring. Status monitoring involves current states or processes of the system. Event monitoring evaluates audit trails, which occurs after processes have finished running. Auditing is provided to evaluate the control structure, assess risk, determine compliance, report on exceptions and make improvements to the system. Systems should be evaluated against the organization's security policies and compliant technical platforms to the security implementation standards.

The monitoring section of a site security plan should include:

- Systems and subsystems to audit
- Tools and configuration settings
- Schedules for periodic auditing tasks
- Review and testing of audit coverage and functionality

Appendix A: Security Policies

In order to obtain a secure system environment, effective information security requires physical, administrative and operational policies combined with solid security and auditing features. Together, these components can protect systems against malicious or accidental access, damage to, or loss of data.

DOE Computer Security Orders

There are two DOE Computer Security Orders: The Unclassified Computer Security Program DOE 1360.2B, and the Classified Computer Security Program DOE 5639-6A-1.

NIST Recommend-ations

Ensuring your organization controls and monitors the security of your systems can be achieved by implementing security policies and procedures that employees can follow. It is critical to document the policies in a site security plan. This plan should be reviewed periodically since networks and resources change rapidly. A small change can open up a site to a larger or completely new risk.

- The National Institute for Standards and Technology (NIST) has defined the following security standards which are called the Minimal Security Functional Requirements for Multi-User Operational Systems. These standards can be used as a baseline for developing your own security policies and procedures:

- Identification and authentication: identifying and validating users through the logon process, and authorization to use systems based on this validation.

- Access control: controlling users access to the network resources and files by setting rights and permissions.

- Accountability and auditing: tracking and logging activities linked to specified users on the network.

- Object reuse: providing multiple users access to individual resources.

- Accuracy: protecting resources from errors, corruption and intrusion.

- Reliability: systems and resources are available and protected against failure or loss.

- Data exchange: securing data transmission over the network.

Appendix B: Logon Banners

Department of Energy

User Warning Notice as defined by DOE classified order 5639.6A-1:

WARNING: To protect the system from unauthorized use and to ensure that the system is functioning properly, activities on this system are monitored and recorded and subject to audit. Use of this system is expressed consent to such monitoring and recording. Any unauthorized access or use of this Automated Information System is prohibited and could be subject to criminal and civil penalties.

Department of Justice

Sample banner from the Department of Justice:

This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.

Glossary

Access Control Entry (ACE). Entries in the ACL that provide information regarding access or auditing permissions to objects for users or groups.

Access Control List (ACL). A list connected to each object specifying various ACEs.

Access Controls. Limits that prevent users from having total access to information systems.

Access token. LSA checks the policy database and retrieves the user rights and other SID information to create the token.

Account domain. Another word for trusted domain.

Backup Domain Controller (BDC). Hold a copy of the security database and user account information in the case of failure of the PDC.

C2 level secure. A level of security for systems defined by the National Computer Security Center (NCSC) of the United States Department of Defense in the trusted computer system evaluation criteria document.

Discretionary access controls. Allowed and denied access control entries in an objects access control list.

Domain. Collection of servers grouped together which share a security policy and a user account database.

File Allocation Table (FAT). File system structure.

Hives. Data located in the four registry subtrees derived from sets of files. The files are either data or log files.

Keys. Value entries contained in the subtrees of the NT registry.

Local Security Authority (LSA). Heart of security subsystem, which validates local and remote logons to all types of accounts.

Logon authentication. Windows NT logon process that verifies user information and authenticates user.

Master domain. Domain configuration consisting of multiple domains and one main master domain.

NT Executive. Provides a set of common services that all environment subsystems can use.

NT File System (NTFS). Windows NT file system structure.

NT Security Model. The foundation of security in the Windows NT OS.

NT server. Software that provides NT OS including extended networking features.

NT workstation. Same piece of software as NT server except is limited to ten simultaneous network connections.

Object ownership. Usually the creator of the object.

Objects. Representation of files, directories, memory, devices, system processes, or threads in the NT operating system.

Permissions. Rules associated with an object describing which access users have.

Primary Domain Controller (PDC). Server in a domain that maintains the security and user account databases for that domain.

Registry. Database that contains applications, hardware, device driver configuration data, network protocols, and adapter card settings.

Resource domain. Another word for trusting domain.

Rights. See user rights.

SAM database. Contains all user and group account information. It is part of the security subsystem which provides user validation services.

Security identifier (SID). A unique ID associated with each user account.

Security policy and procedures. An organization's statement about how it will provide security, handle intrusions, and recover from damage caused by security breaches.

Security policy for domains. Consists of password policies and account lockout policies.

Security Reference Monitor (SRM). Part of security subsystem responsible for enforcement of access validation and audit generation policies required by the LSA.

Security Subsystem. The combination of the logon processes, LSA, SAM, and SRM in the NT security model.

Server. The piece of hardware in a client/server environment that holds software and hardware shared among its clients.

Shares. Sharing of files and directories over the network.

Subject. The user's access token connected with each process the user runs.

Trusted domain. Makes accounts available for use in the trusting domain.

Trusting domain. Contains the resources the trusted domain will access.

Trusts. An administrative way to link together two domains allowing one domain's users access to the other domain.

User account database. Holds account information for all users that can log into a domain.

User authentication. Determined by validation of the SAM database to the user logon information.

User rights. Authorization to perform specified actions on a system.

Workgroup. A single system or multiple systems that are not connected to a domain.