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

Form SF298 Citation Data

Report Date *("DD MON YYYY")* 01121997	**Report Type** N/A	**Dates Covered (from... to)** *("DD MON YYYY")*

Title and Subtitle Window's NT Network Security A Manager's Guide	**Contract or Grant Number**
	Program Element Number
Authors	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) IATAC Information Assurance Technology Analysis Center 3190 Fairview Park Drive Falls Church VA 22042	**Performing Organization Number(s)**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Monitoring Agency Acronym**
	Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms	
Document Classification unclassified	**Classification of SF298** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** unlimited
Number of Pages 22	

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	12/1/97	Report

4. TITLE AND SUBTITLE
Window's NT Network Security A Manager's Guide

5. FUNDING NUMBERS

6. AUTHOR(S)
Marcey Kelley, Wendall Mayson

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IATAC
Information Assurance Technology Analysis
Center
3190 Fairview Park Drive
Falls Church VA 22042

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
DTIC-IA
8725 John J. Kingman Rd, Suite 944
Ft. Belvoir, VA 22060

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

This document outlines NT security mechanisms, discusses teminology, provides a generic security model, discusses designing the NT environment including trusts and domains, group management, managing NT file systems, and monitoring system activities.

14. SUBJECT TERMS
Network Security, CIAC

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	UNCLASSIFIED	UNCLASSIFIED	None

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.

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.

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

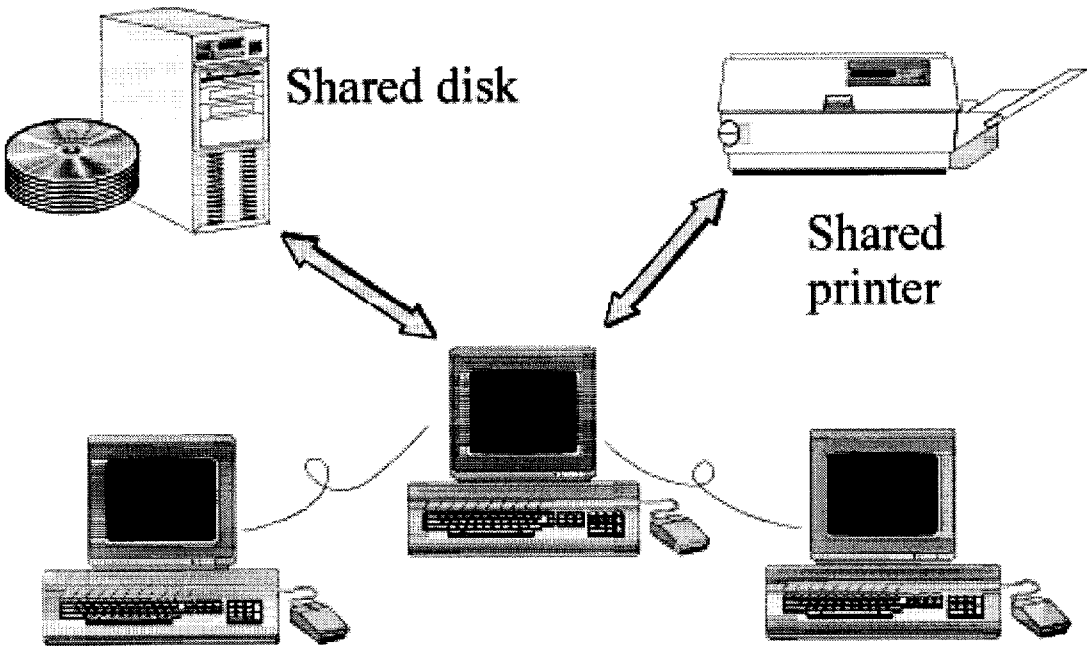
There are two different types of Windows NT software available: Windows NT Workstation and Windows NT Server. The Server version is the same as the Workstation version except that it provides additional features for networking. Only ten users can access a Windows NT Workstation at a time, and NT Server 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 Subsystem

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.

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

- Local Security Authority (LSA)

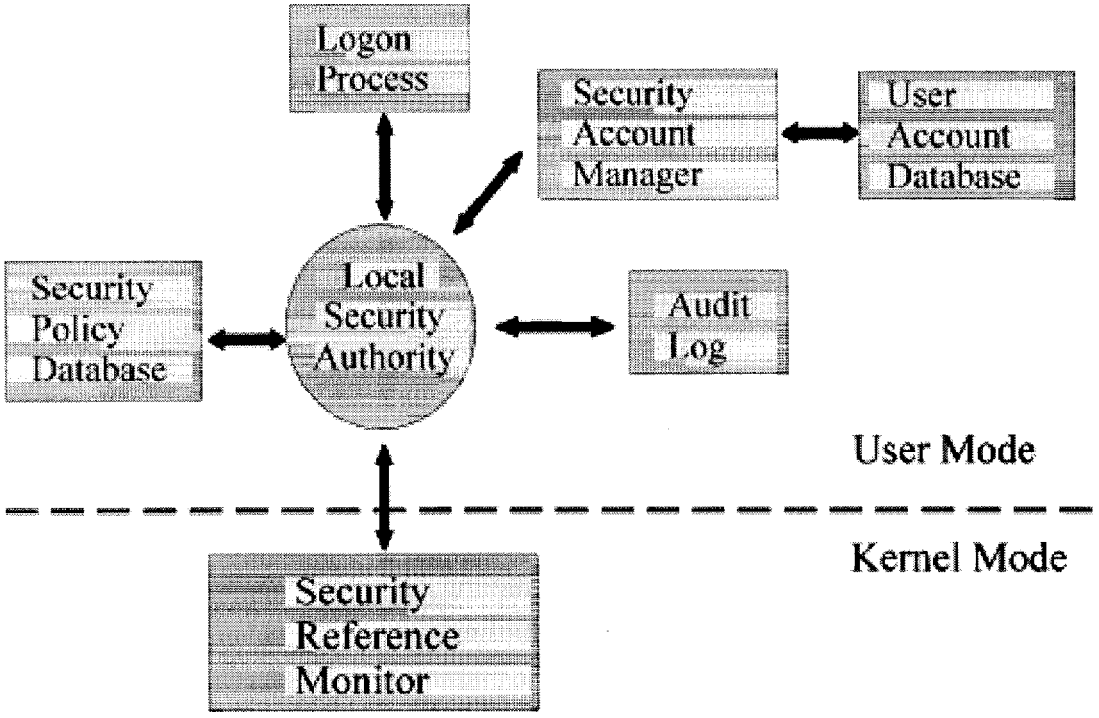
- Security Account Manager (SAM)
- Security Reference Monitor (SRM)

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.

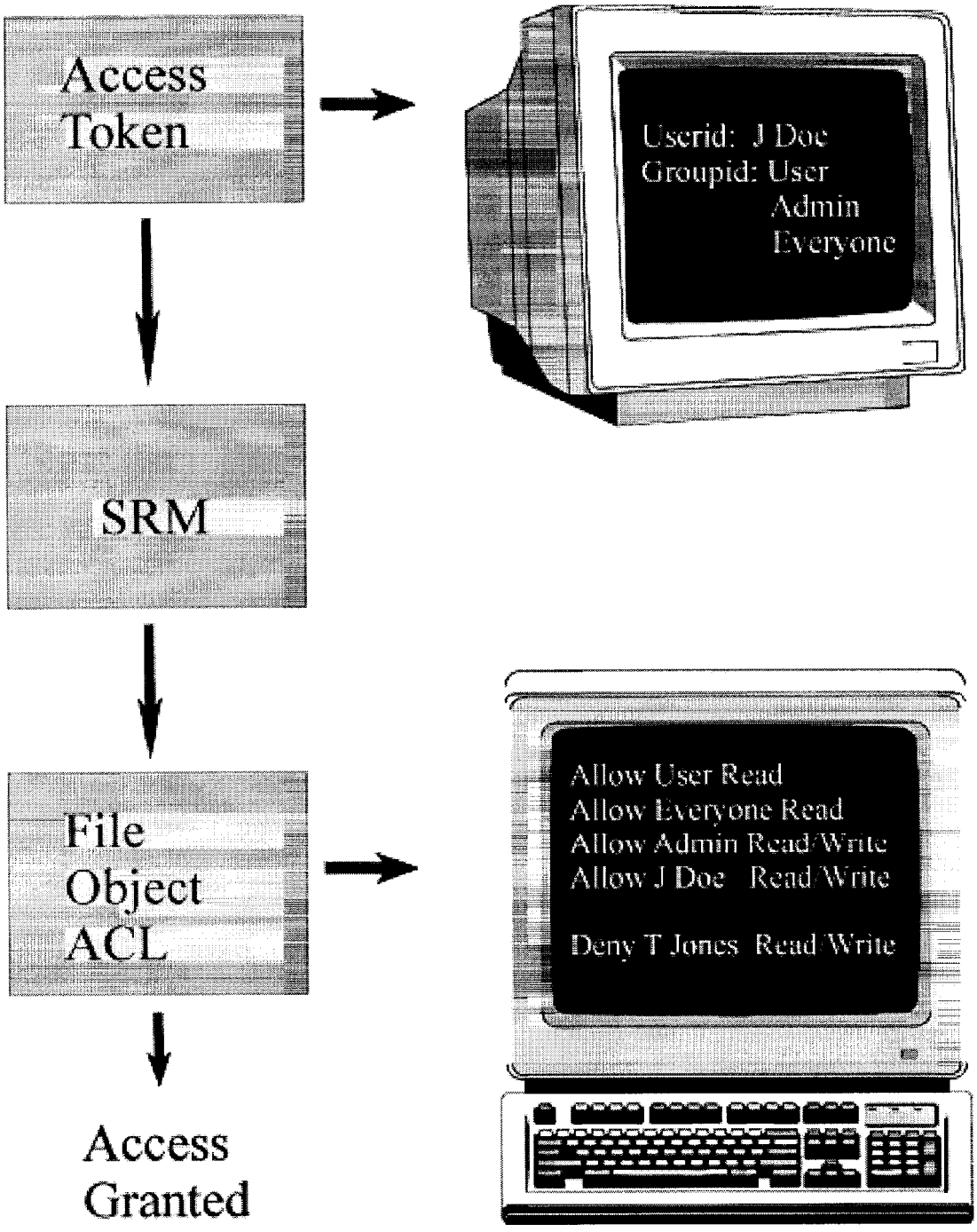
Security Reference Monitor (SRM)

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 users 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 ***We/come*** 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 ***We/come*** 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:

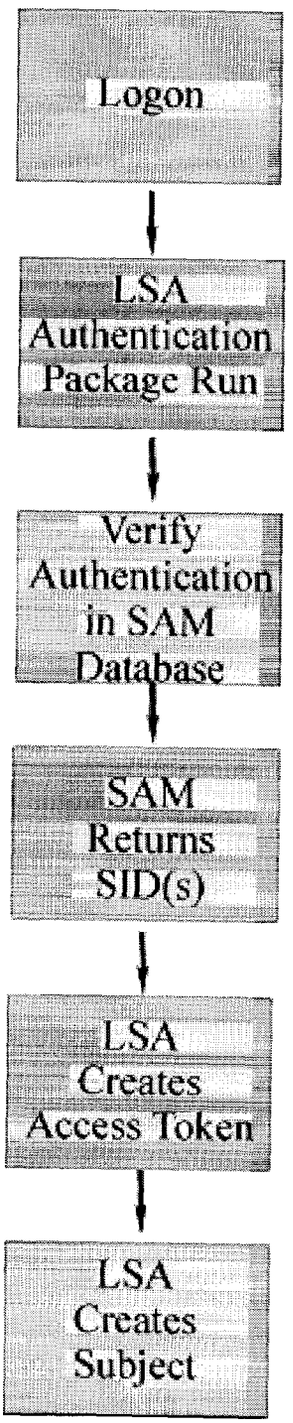
A ***We/come*** dialog is displayed which requires a user name, password and the server/domain the user would like to access. If the user information is valid, the system proceeds to authenticate the user.

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

SAM does a comparison between the user logon information and the servers 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 users request.



• Figure 4: NT Logon Process

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.

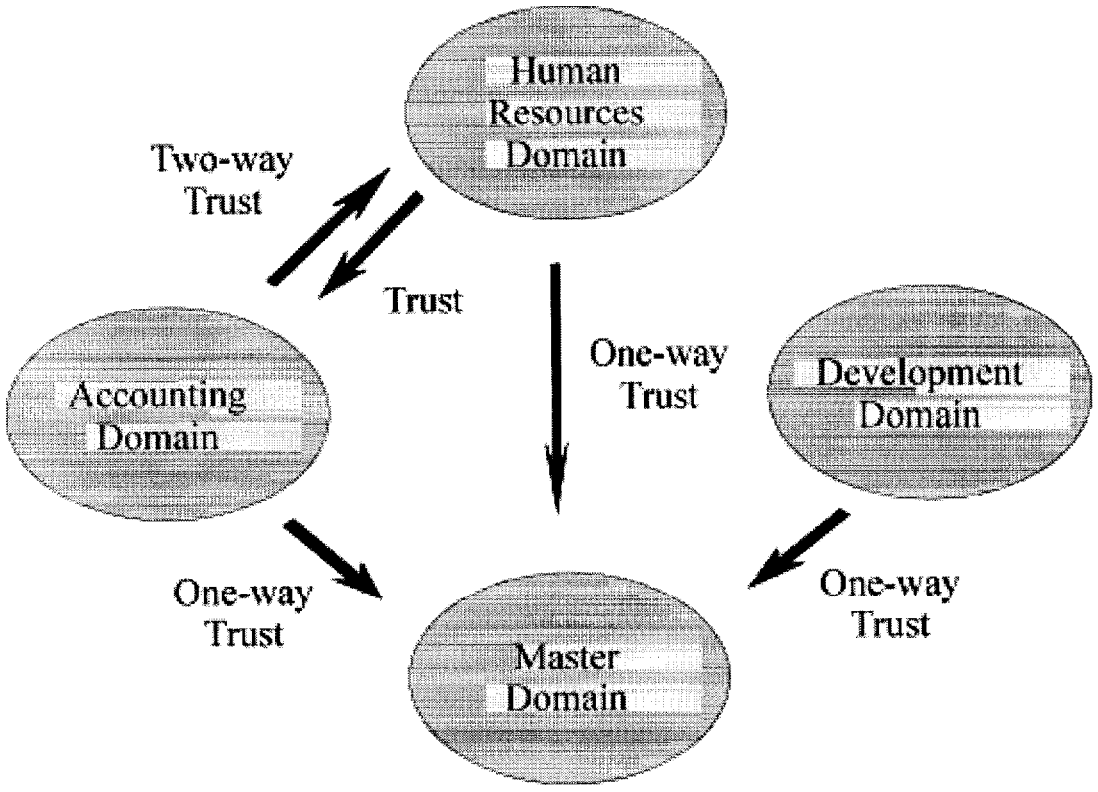
Trust Relationships

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:

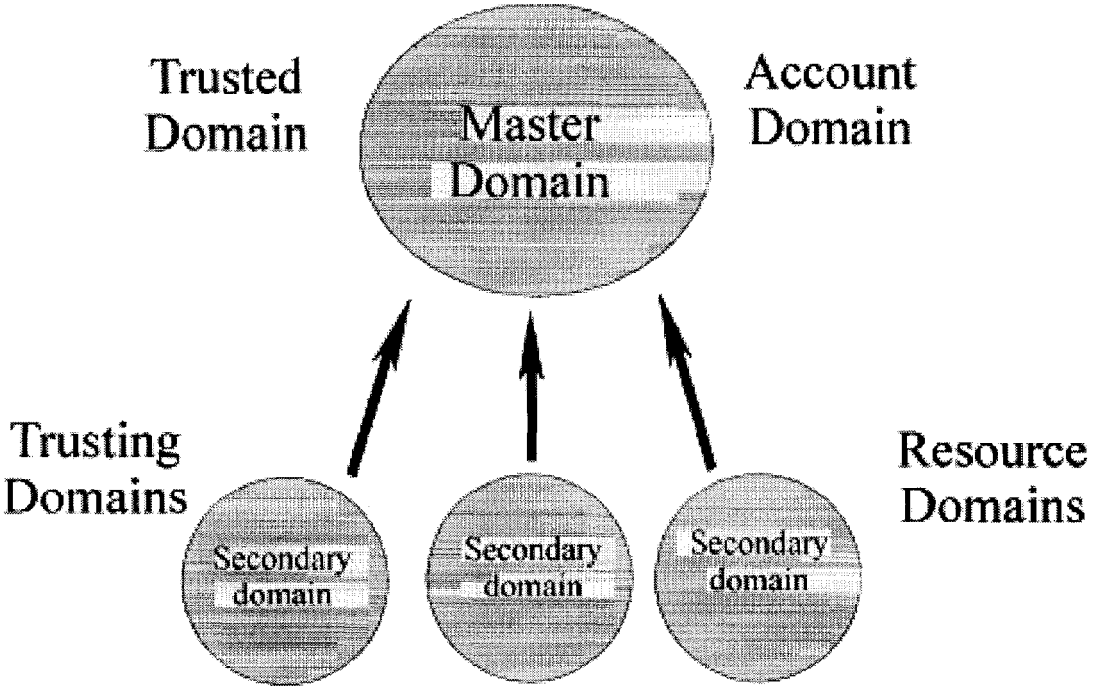
- Single Domain
- Master Domain
- Multiple Master Domain

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.

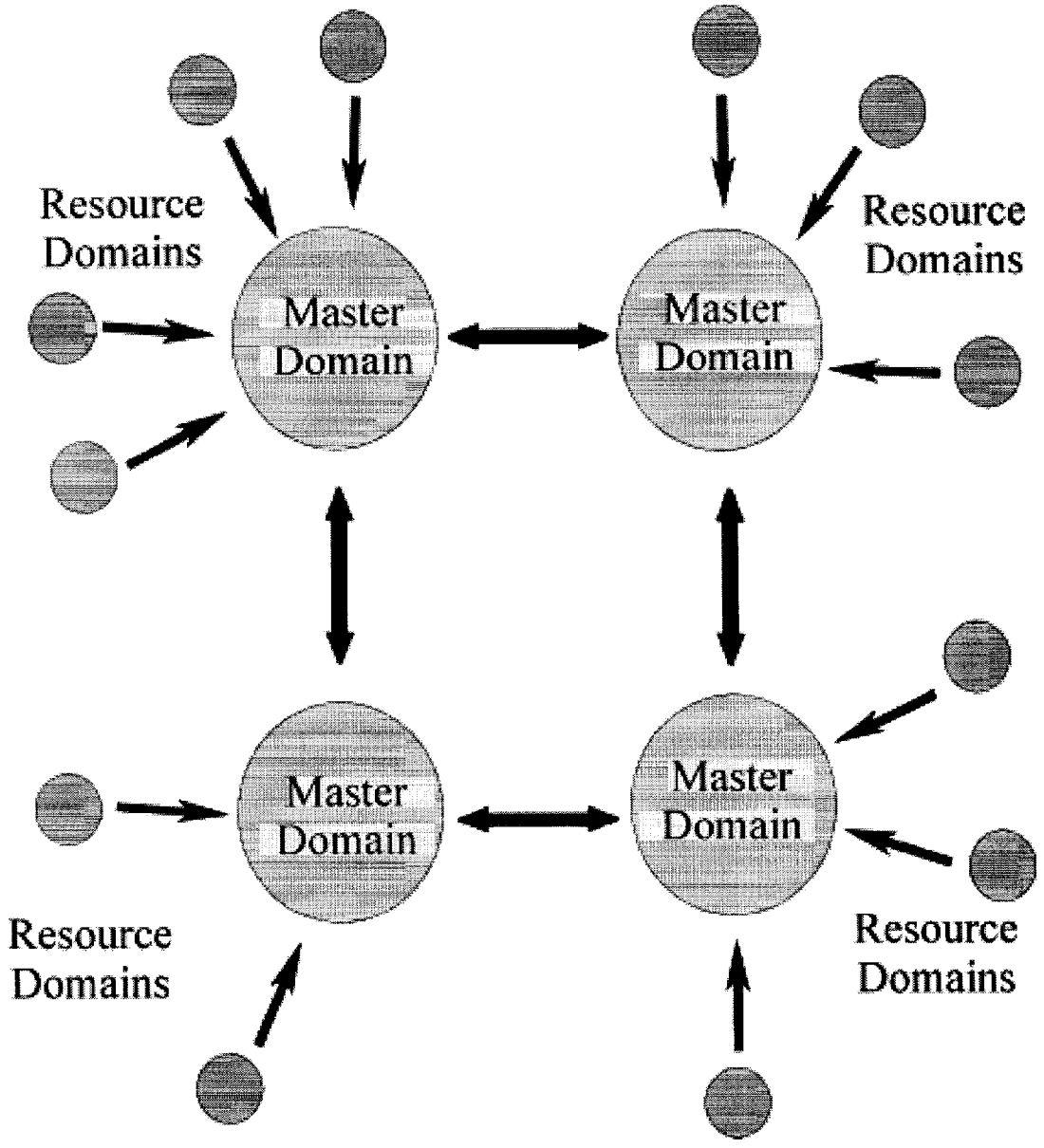
Resources are managed locally on the trusting domains, while user accounts are controlled on the trusted master domain. The master domain model is used in organizations with less than 10,000 users. The number of users is limited because the accounts are all maintained on the master domain.



• 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.

M u . 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

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.
- Sewer 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 users 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.