NCSC '94

Seventeenth National
Computer Security Conference

Windows NT Security

Presented by:

Jeff Williams

Arca Systems, Inc.
8229 Boone Blvd., Suite 610
Vienna, VA 22182
(703) 734-5611

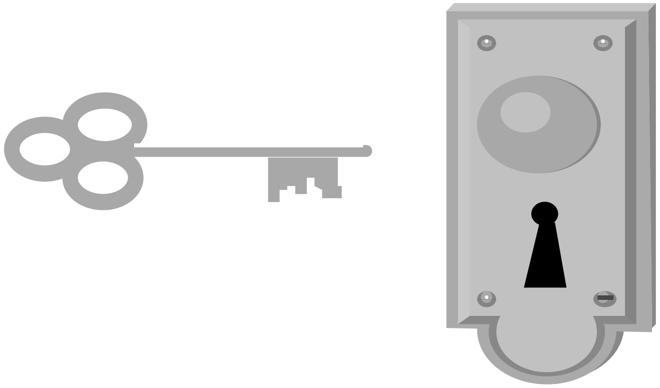
Session Objectives

- After attending this session, you should be able to describe:
- What Windows NT™ Advanced Server is and how it works
- Describe the fundamental security features of Windows NT™ Advanced Server
- Describe appropriate configurations and/or procedures for achieving security control with NT Advanced Server

* Windows NT is a registered trademark of Microsoft Corporation. All instances of Windows NT (including NTAS) in this session shall be considered as including the Microsoft trademark (TM) by reference.

Session Outline

- Windows NT™ Overview
- The NT™ Advanced Server
  - What is it?
  - How does it work?
- Basic Security Features
  - User Accounts and Groups
  - Authentication
  - Rights and Abilities
  - Permissions
  - Auditing
  - Availability
- Viruses and Windows NT™ Advanced Server



What is Windows NT?

- Microsoft's next generation 32-bit operating system
- Provides secure, authenticated access to network resources from a variety of platforms
- Borrows from five basic operating system models
  - Client / Server
  - Object
  - Layered
  - Symmetric Multiprocessing
  - Pre-emptive Multi-tasking
- Two products
  - Windows NT Client
  - Windows NT Advanced Server (NTAS)

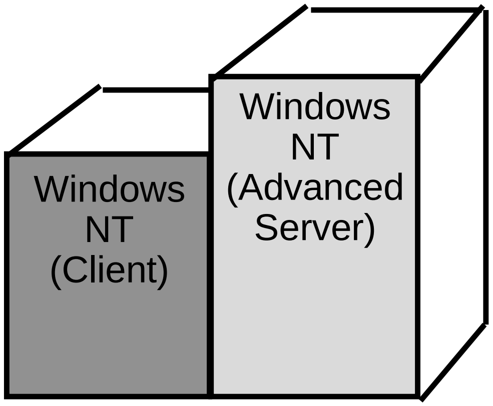
An Important Note

- This presentation covers Windows NT™ 3.1, the current release
- The next (imminent) release, Daytona™, will have additional security features (not covered in this presentation)
- Cairo™ release will offer even more security features

NTAS Compared to NT Client

NTAS is optimized for network resource management, security and performance

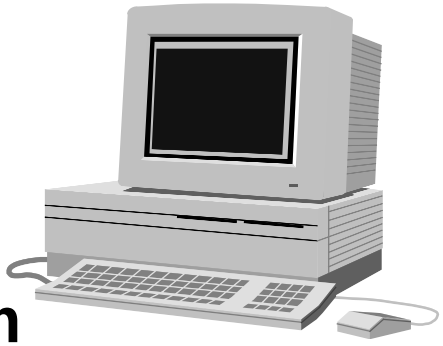
- NTAS adds
  - domain users
  - global groups
  - additional user rights and restrictions
- Administration tools for
  - domains
  - domain services
  - trust relationships
  - clients and servers
- More audit events



NT = .85 NTAS

NTAS Compared to NT Client (continued)

- Disk functions are expanded
- Centralized creation and storage of domain user profiles
- Built-in services for Macintosh clients
- Expanded remote access service (RAS) (64 lines)
- Higher performance hardware platform capable (up to 4 symmetric processors)



NT Advanced Server Overview

- NT Advanced Server is for workstations
  - Latest Windows desktop environment
- Runs existing applications
  - MS Windows (16 and 32 bit)
  - MS-DOS
  - MS OS/2
  - POSIX
- Many Supported Microprocessors
  - x86
  - RISC
- Connects to existing networks
  - Banyan® VINES®
  - Novell® NetWare®

NT Advanced Server Communication

- Networking is built in
  - Peer-to-Peer networks supported between NT Clients
  - Domains (with NT Advanced Server)
  - Remote access support
- Mail
  - Workgroup Postoffice handles mail between NT systems
  - Support for OLE
- File and Directory Sharing
  - Files and directories can be shared
  - Directory Replication distributes workload

NT Advanced Server Security

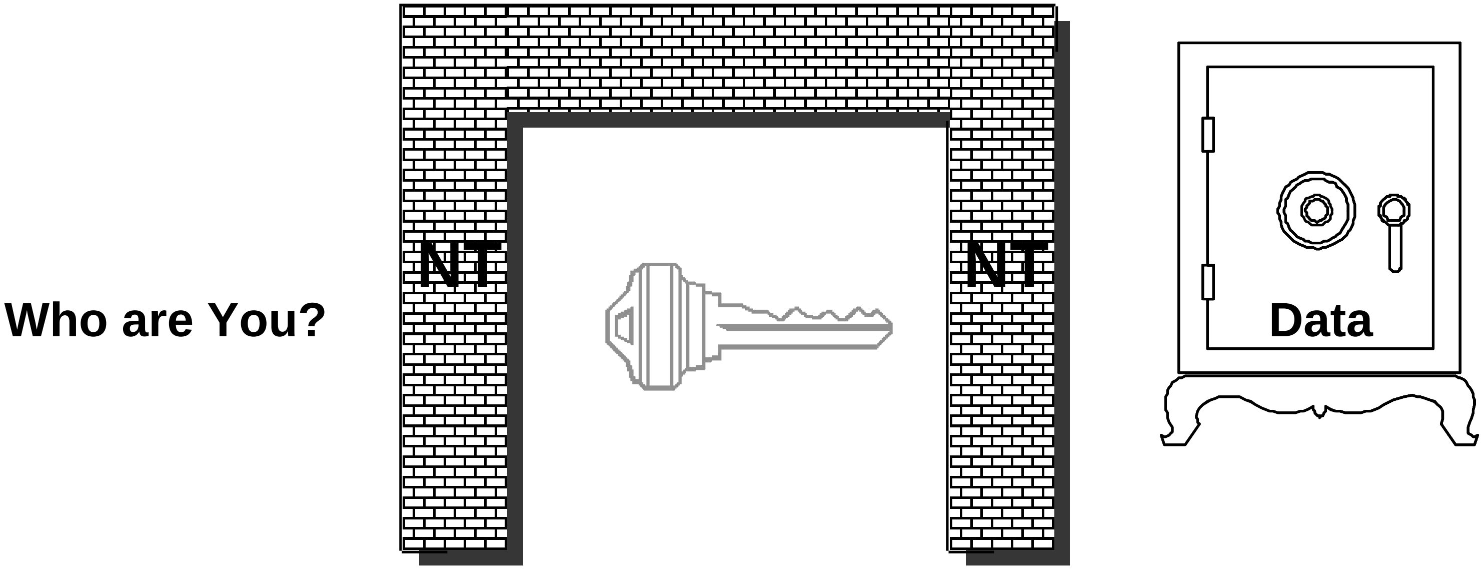
- Advantages
  - Strong authentication at the workstation
  - Access control through permissions
  - Auditing
  - Central security administration
- Security Disadvantages
  - Many security features are not enabled
  - Limited assurance

Windows NT Security Approach

NT attempts to strike a new balance between "user-friendly" and security

<u>Distributed security approach through controls on</u>

- *Users* (mainly through assignment of users to groups)
- *Accesses to resources* (through permissions)



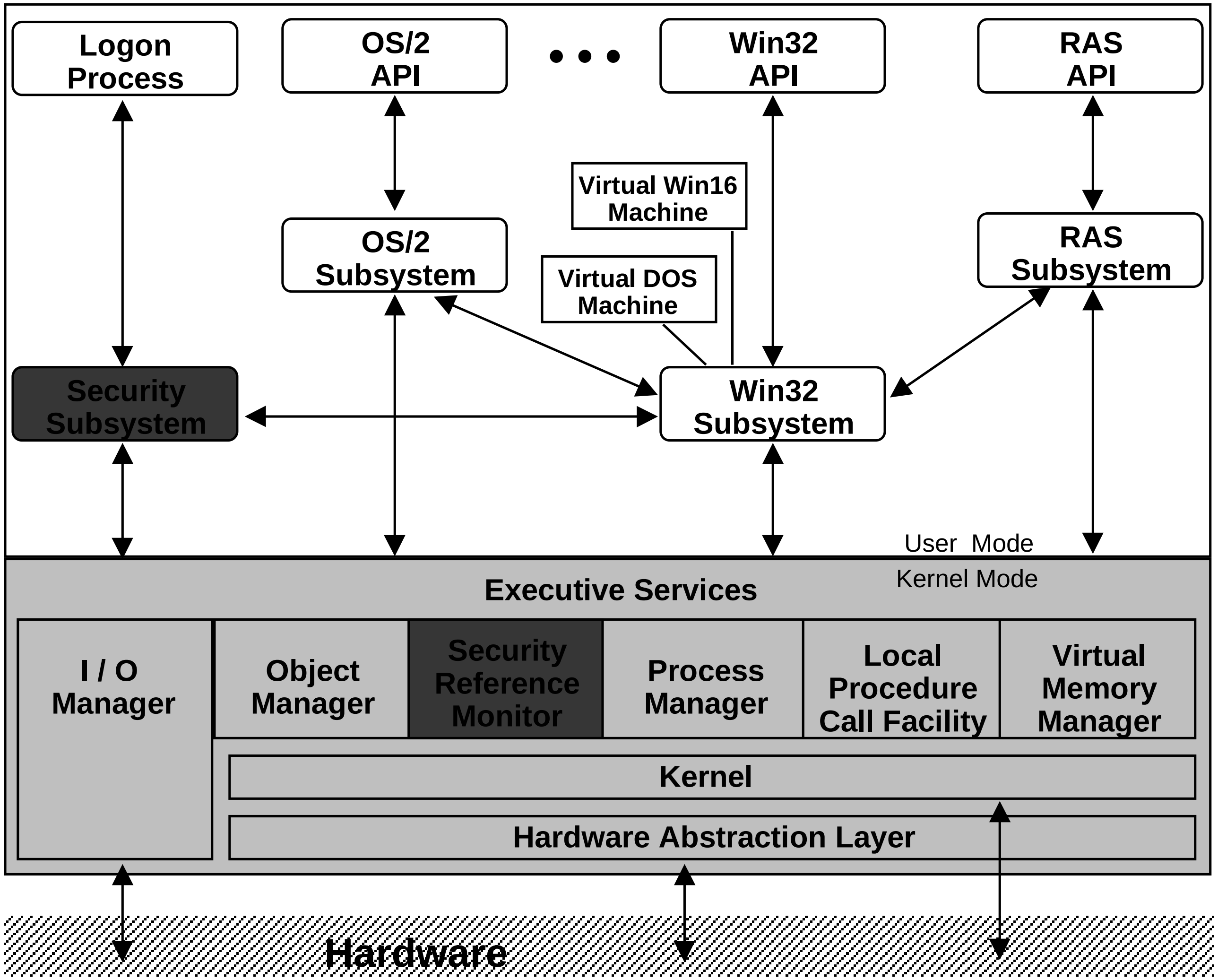
How Strong is Windows NT Security?

- The security implications of much NT functionality are not currently well understood
- General security principle: the more functionality, the greater number of exposures there will be (and NT has a great deal of functionality for a LAN product!)
- Another general security principle: the more connectivity, the more ways there are to gain unauthorized access (and NT is extremely connectivity-capable)

How Strong is Windows NT Security?

- The technology of achieving unauthorized access to systems connected to networks is advanced and ever-increasing
- BUT
- There is little evidence that the “cracker” community has targeted NT networks *so far*
- Overall assessment of NT security capability - somewhere between correctly configured Unix and VMS *if security capabilities of NT are turned on*
- Problem: “Out-of-the-box” NT does not have security capabilities turned on. *You have to work to make NT secure!*

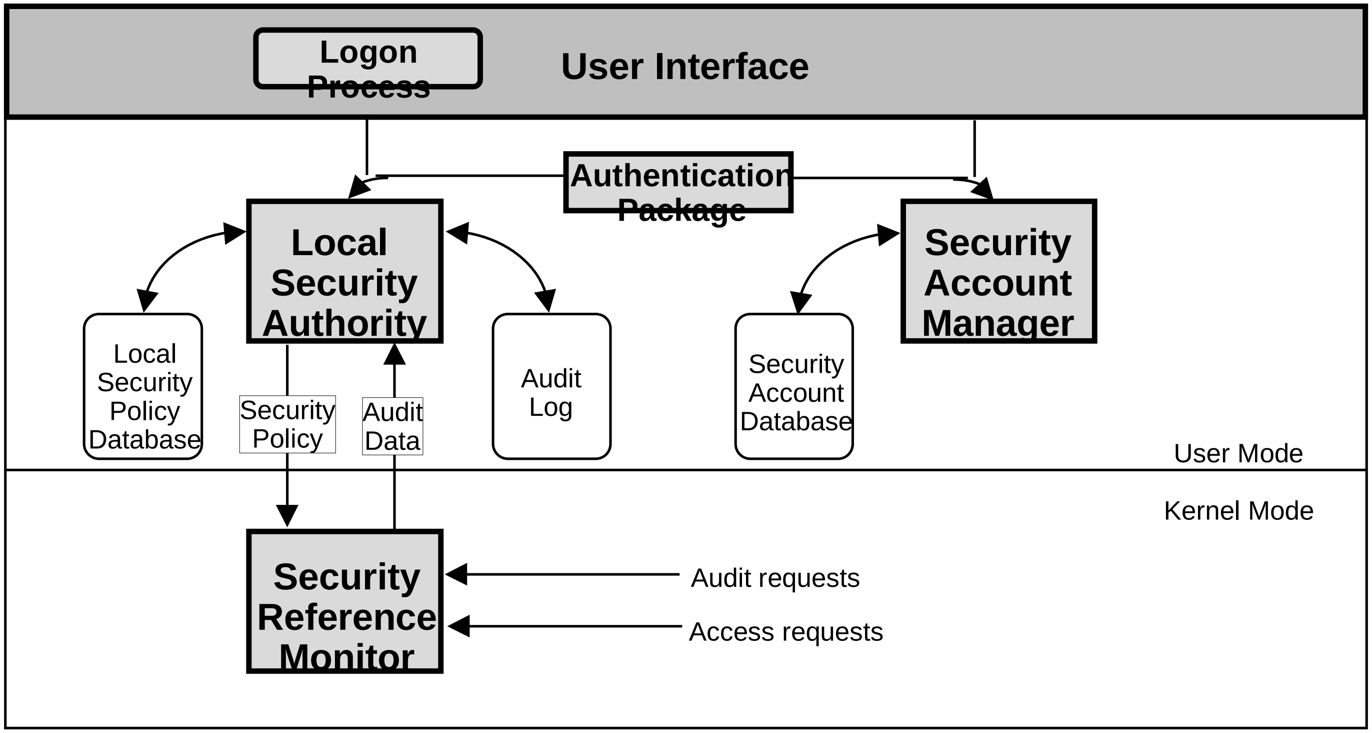
Windows NT Architecture



API = Application Program Interface

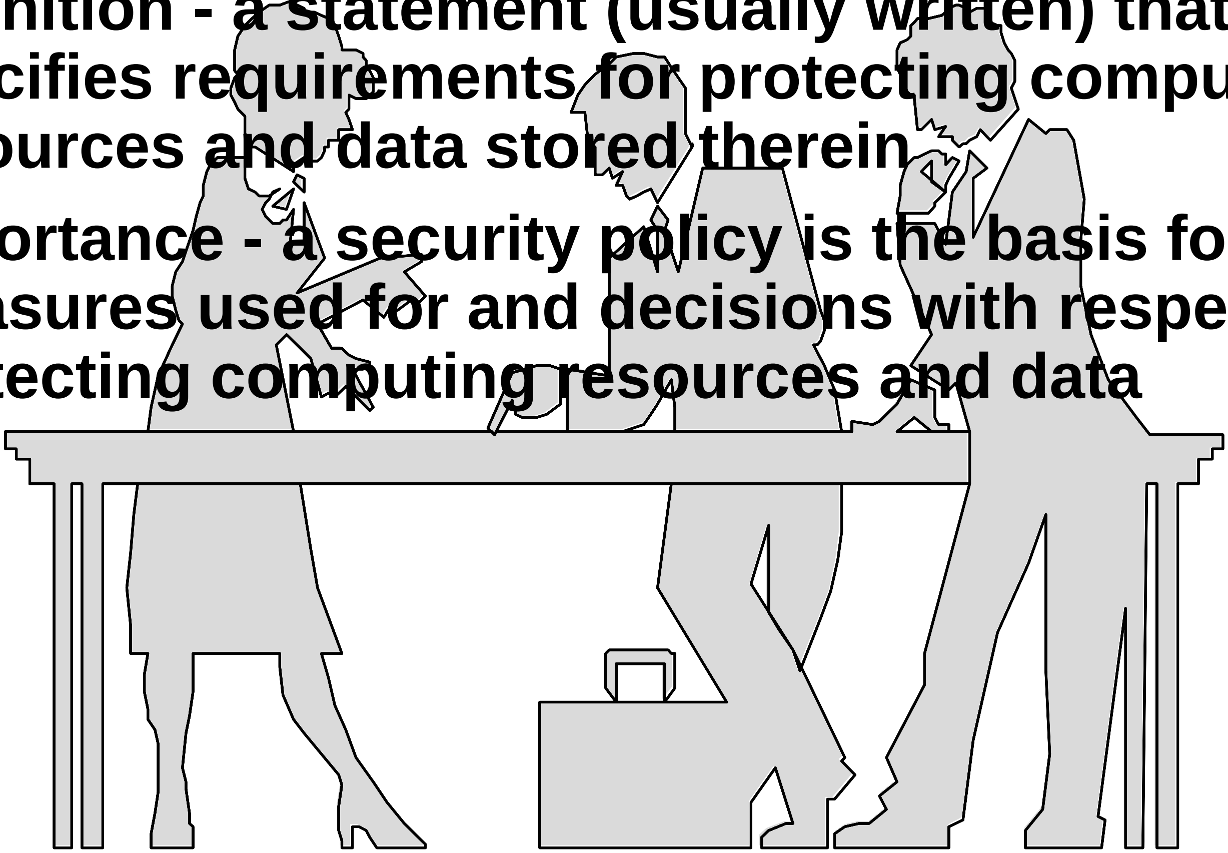
NT Security Components

- **Security Subsystem (“Local Security Authority”)--ensures the logon process**
- **Security Reference Monitor--mediates *every* access to objects by subjects**



Security Policy

- Definition - a statement (usually written) that specifies requirements for protecting computing resources and data stored therein
- Importance - a security policy is the basis for all measures used for and decisions with respect to protecting computing resources and data



Arca Systems
Leaders in Security Integration

Topics Often Addressed

- Who is authorized to use the system?
- What are the users’ rights?
- What resources do users need to access?
- What types of passwords can/cannot be chosen by users?
- What level of user accountability is required?
- How much auditing should be turned on?

- Remember: NT supports only certain policies

The "Bottom Line"

Windows NT has many security features that support a security policy. As shipped by Microsoft, however, NT security features are, for the most part, not turned on. To get the security you need, <u>you</u> must turn these features on!

Outline of Basic Security Features

- User Accounts and Groups
- Authentication
- Rights and Abilities
- Permissions
- Auditing

NT Client Accounts

- User accounts
  - Are *local*--allow access to the NT Client
  - *Do not* allow access to server resources (although one can logon to NT Client, then do a netlogon to the NT network)
- Administrator and Guest built-in accounts
- Built-in accounts come preconfigured with local group memberships
- One can create other accounts as needed

NT Advanced Server Accounts

- Local and global (or domain) accounts
- Two built-in local accounts
  - Guest (not initially turned on)
  - Administrator
- Built-in accounts come preconfigured with local and global group memberships
- Create other accounts as needed
  - local and domain users
  - other types of administrators (e.g., Security Admins)

About NT Groups

- **Users can only perform the actions allowed by the specific rights and abilities of the groups to which they belong**
- **Users can (and typically do) belong to more than one group**
- ***Users belonging to groups with different rights and abilities effectively have the rights and abilities of the “most powerful” group to which they belong!***

Global Groups

- Simplify domain accounts administration
- Are EXPORTABLE to other computers for inclusion in their local groups
- Can contain
  - only domain user accounts from the home domain
  - no other global groups or local groups
- Can be directly assigned access rights
  - however, it is easier to assign and administer rights to local groups in which global groups are members

Local Groups

- Simplify local account administration
- Defined only for one computer’s resources
- Can contain
  - domain user accounts
  - local user accounts
  - global groups
- Assigning rights directly to local groups treats global group members like any other user account

WARNING: Be careful when including global groups in local groups!

- *you may be extending trust too far*
- *actual identities of global users may not be known - it is best to view individual names of users in global groups*

NT Client Built-in Groups

- Local groups only
- Built-in groups
    - Administrators
    - Power Users
    - Users
    - Guests
    - Backup Operators
    - Replicator
    - Other “Special Groups”
- Preconfigured rights and abilities
- Create and configure other groups as desired

NTAS Built-in Groups

- Local and global
- NTAS built-in groups
  - Administrators
  - * Domain Admins
  - Users
  - * Domain Users
  - Guests
  - Account Operators
  - Backup Operators
  - Print Operators
  - Server Operators
  - Replicator
  - Other “Special Groups”

* the only Global Groups

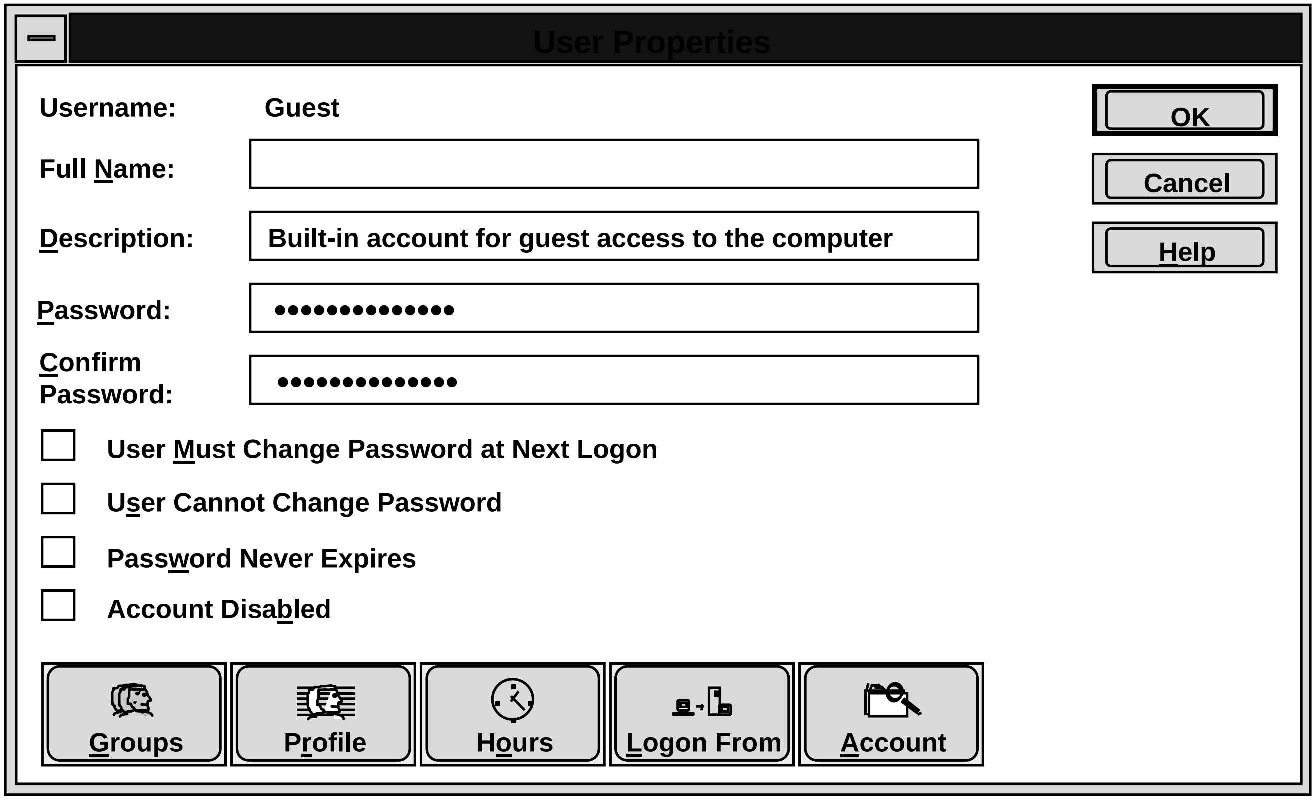
Configuring NTAS Groups for Security

- In general, each user should be a member of the Users group, but not groups with higher levels of privileges
- Limit membership in Administrator and Power Users groups

NT Authentication

- *Authentication* means establishing that a user is who s/he claims to be
- The NT authentication process involves
  - User name
  - Password
- The user is prompted to press CRTL-ALT-DEL before a logon panel is presented
  - Ensures that the Security Subsystem Logon Process controls the login(“Secure Logon”)
  - Some processes bypass the Secure Logon
- Passwords are protected in several ways
  - Encryption
  - Stored in non-publically accessible location

Logon Password Options



User Properties

Username: Guest

Full Name:

Description: Built-in account for guest access to the computer

Password: ••••••••••••••

Confirm Password: ••••••••••••••

☐ User Must Change Password at Next Logon

☐ User Cannot Change Password

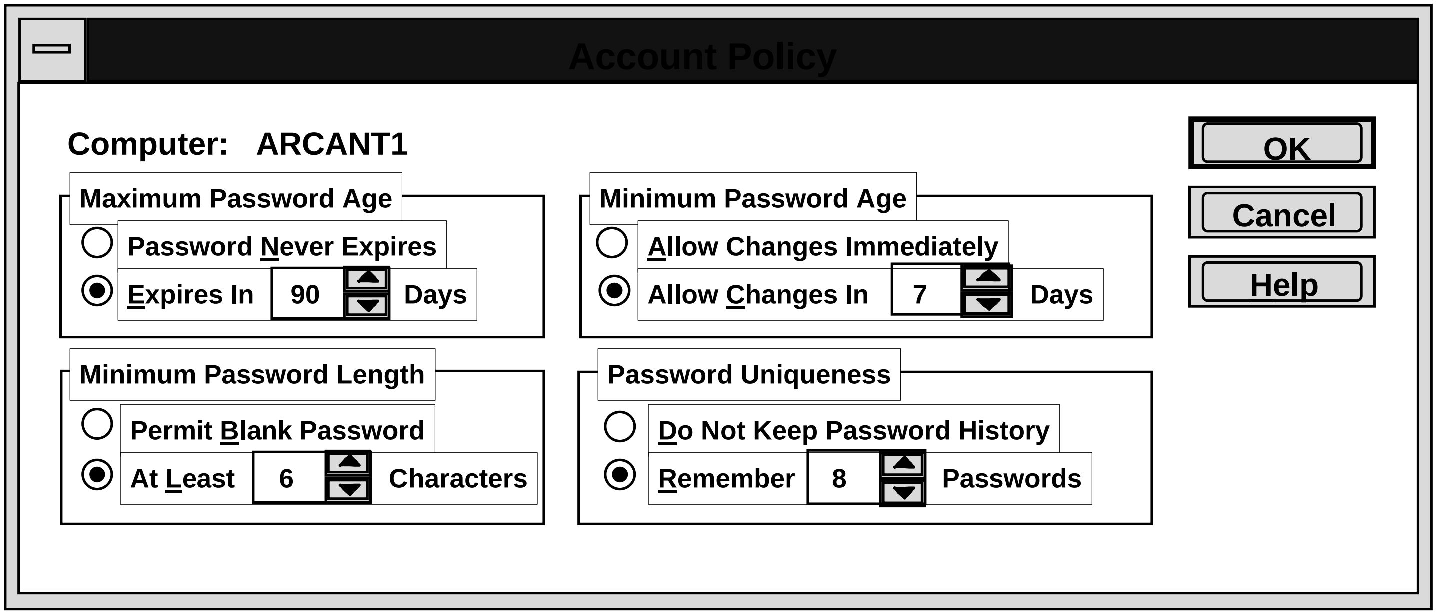
☐ Password Never Expires

☐ Account Disabled

NT Password Policy

Controls logon passwords for all accounts managed by this computer

- **Maximum Age**
- **Minimum Length**
- **Minimum Age**
- **Uniqueness**



Computer: ARCANT1

Maximum Password Age
○ Password Never Expires
● Expires In 90 Days

Minimum Password Age
○ Allow Changes Immediately
● Allow Changes In 7 Days

Minimum Password Length
○ Permit Blank Password
● At Least 6 Characters

Password Uniqueness
○ Do Not Keep Password History
● Remember 8 Passwords

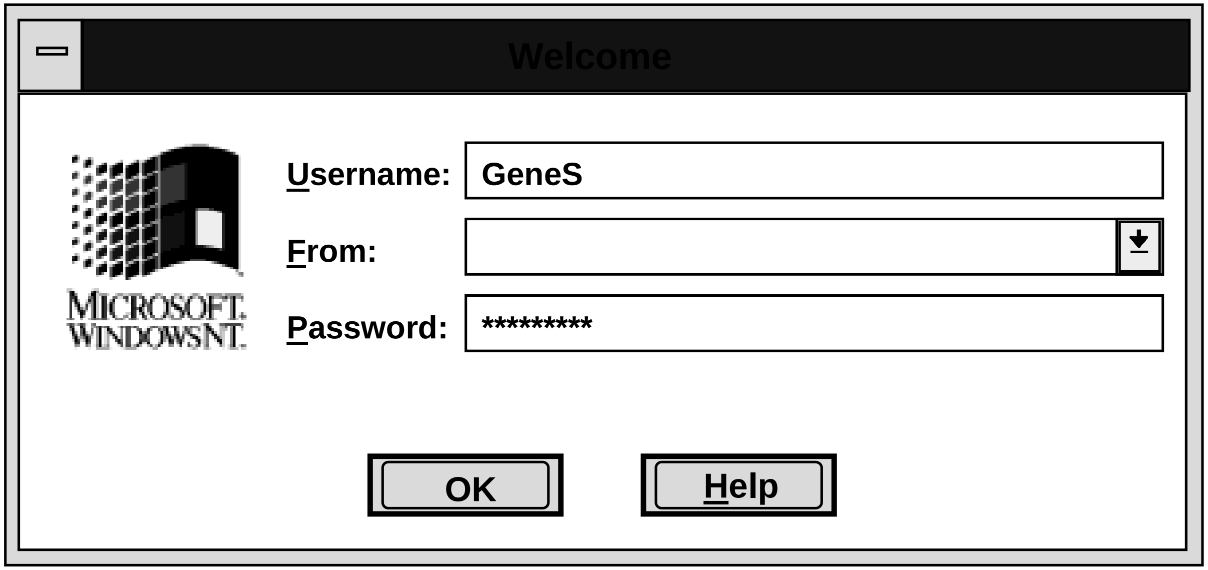
Recommendations for Password Security

- Use policy options, as appropriate
  - Password Age option limits value of stolen passwords
  - Password Length option can help make passwords less guessable
  - Minimum Password Age and Password Uniqueness options can prevent users from immediately changing new passwords to previous ones
- *Do not* use "Permit blank password" option
- Important note: the current NT release does not have account lock feature after a criterion number of unsuccessful logons, so using the password policy options appropriately is especially important!

Secure Logon

Why does NT provide a secure Logon?

- Multiple users can securely share same computer
- Forces users to identify who they are, and prove it
- Single logon password for NTAS based systems



Username: GeneS

From:

Password: *********

Authentication

- Local logon works through Local Security Authority
- Netlogon authenticates against the Security Accounts Manager on an NTAS
- Passthrough authentication works for other domains
- Non-NT logon is supported, but less secure
- Remote Access authentication is separate

Remember: The more ways to logon, the more ways to break in!

Rights

- Rights authorize a user to perform certain actions relative to the system as a whole
- Selectable in NT User Rights Policy administration tool

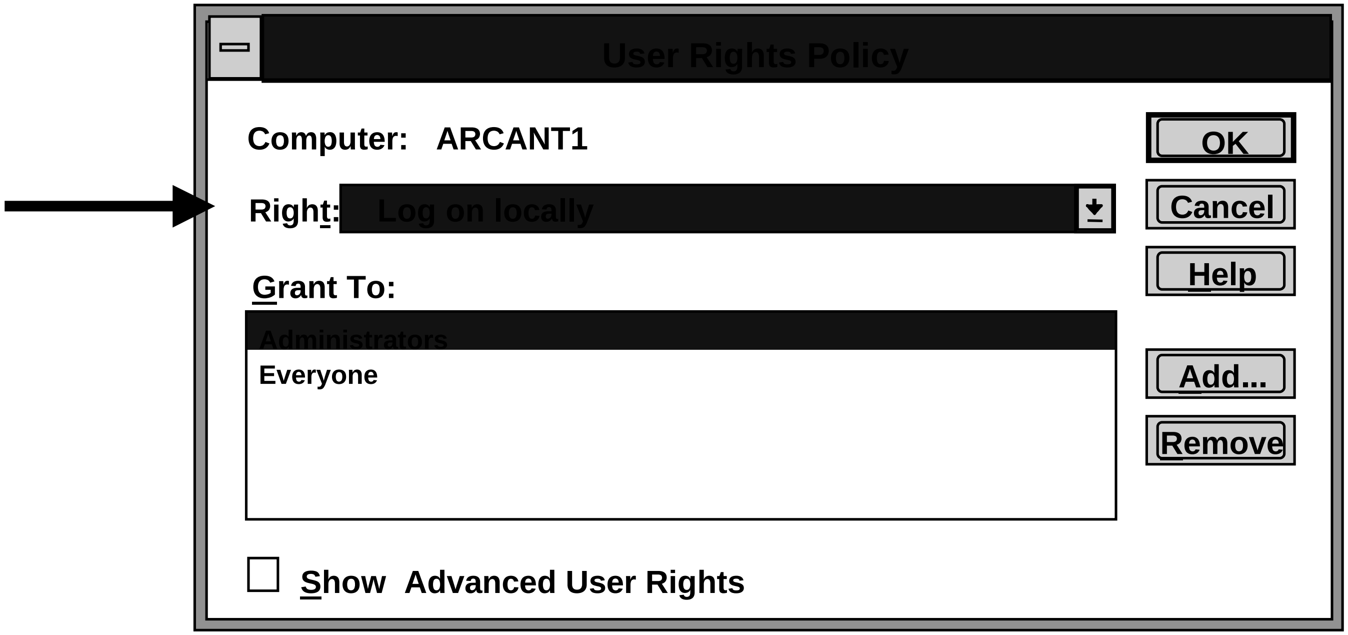
Be aware that some rights can override permissions!

NT Advanced Server Rights

- Logon Locally
- Access this computer from network
- Take ownership of files
- Manage auditing and security log
- Change the system time
- Shutdown the system
- Force shutdown from a remote system
- Backup files and directories
- Restore files and directories

User Rights Policy

- Implements the rights portion of the “rights vs. permissions” NT access control model
- Rights assigned to each user and group defines the User Rights policy that NT will enforce



Computer: ARCANT1

Right: Log on locally

Grant To:

Administrators

Everyone

□ Show Advanced User Rights

Abilities

- “Abilities” authorize a user to perform certain additional actions beyond those granted via Rights
- Membership in groups automatically conveys abilities to users
- Abilities are indirectly administered by the rights you grant to groups

NT Advanced Server Abilities

- Create and manage user accounts
- Create and manage local groups
- Assign user rights
- Lock the workstation
- Override a workstation’s lock
- Format a workstation’s hard disk
- Create common groups
- Keep a local profile
- Share and stop sharing directories
- Share and stop sharing printers

Summary of NTAS User Rights & Abilities

Rights	Admins	Server Operators	Account Operators	Print Operators	Backup Operators/ Replicator	Everyone	Power Users	Users	Guests
Log on locally	•	•	•	•	•	ø	ø	ø	ø
Access system from network	•					•	ø	•	•
Take ownership of files	•								
Manage audit, security logs	•								
Change system date, time	•	•					ø		
Shutdown system locally	•	•	•	•	•	ø	ø		
Shutdown system remotely	•1	•					ø		
Backup files & directories	•	•			•				
Restore files & directories	•	•			•				
Abilities									
Create, manage user accounts	•		•2				ø 3		
Create, manage global groups	•		•2						
Create, manage local groups	•		•2				ø 2	•4	
Assign user rights	•								
Lock the system	•	•				•5	ø		
Override lock on system	•	•							
Format system's hard disk	•	•							
Create common groups	•	•					ø		
Keep local profile	•	•	•	•	•		ø		
Share, stop sharing directories	•	•					ø		
Share, stop sharing printers	•	•		•			ø		

• = right is granted to this group
ø = applicable to NT clients only
(blank means not applicable)
1 = feature is unimplemented

2 = Cannot create or change admins or operators accounts or groups
3 = Can only change or delete user accounts created by this person
4 = Applicable only for groups they create, if they can logon locally
5 = Only applicable if granted local logon right

Arca Systems
Leaders in Security Integration

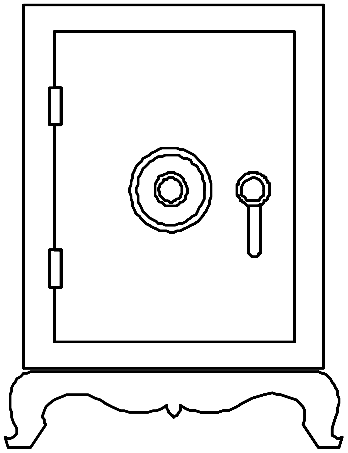
Configuring Rights and Abilities

- Generally be stringent in assignment of rights to groups
- Learn more about which abilities go with which particular rights--*many rights include a wide range of abilities*
- Limit use of guest account--has many built-in rights and abilities on an NT Advanced Server
- Perform regular/periodic reviews
  - Group memberships
  - Rights assigned to groups

NT Permissions

Setting appropriate permissions is one of the most powerful methods of elevating system security

- **Permissions control accesses to NT system resources**
- **“Owners” set permissions**
- **NT permissions authorize a user or group to perform specific types of accesses**



How NT Controls User Accesses

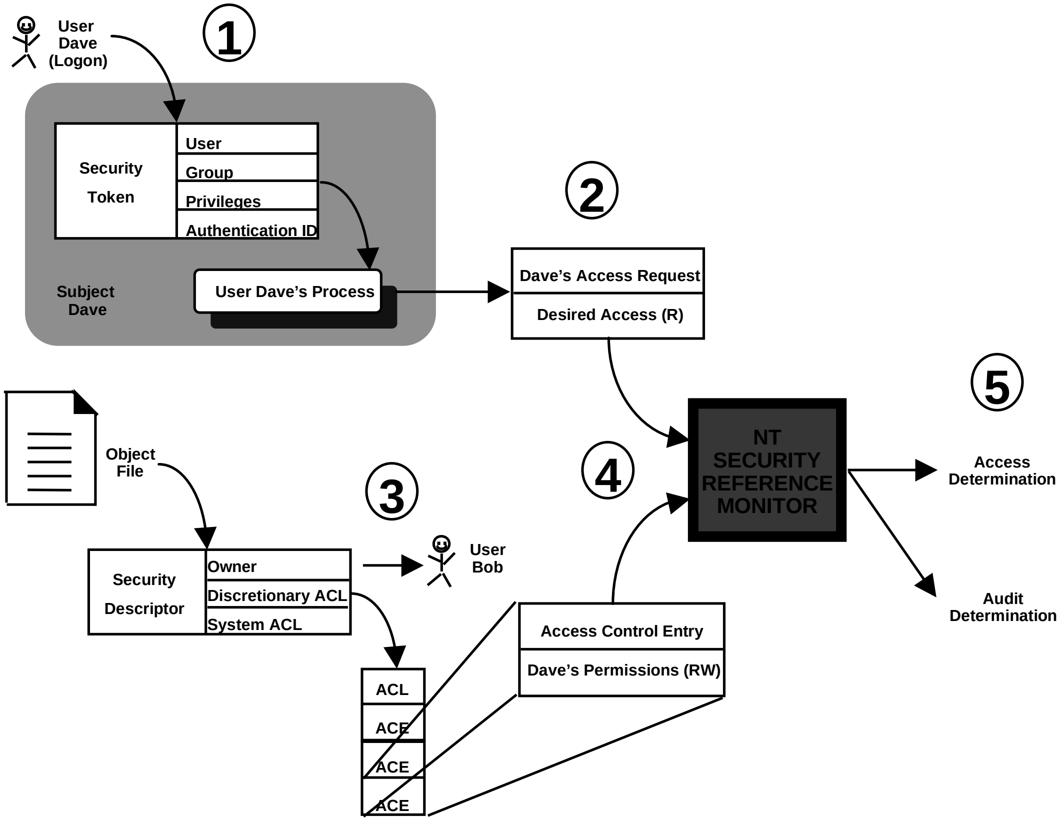
Security Reference Monitor

Compares

- **Requested permissions in User's access token**
- **With permissions associated with requested object**

Grants or denies access to object based on

- **Permissions match or mismatch**

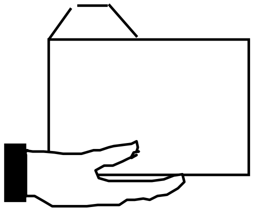


File and Directory Permissions

- File permissions
  - No Access = (none)
  - Read = (RX)
  - Change = (RWXD)
  - Full Control = (All)
- Directory permissions
  - No Access = (none)(none)
  - List = (RX)(not specified)
  - Read = (RX)(RX)
  - Add = (WX)(not specified)
  - Add & Read = (RWX)(RX)
  - Change = (RWXD)(RWXD)
  - Full Control = (All)(All)

File Sharing Permissions

- File sharing enables sharing of files and directories with network users
- File sharing permissions are separate from and in addition to NTFS permissions
  - Full Control (All)
  - Change (RWXD)
  - Read (R)
  - No Access (none)



- Only Admins can set share permissions

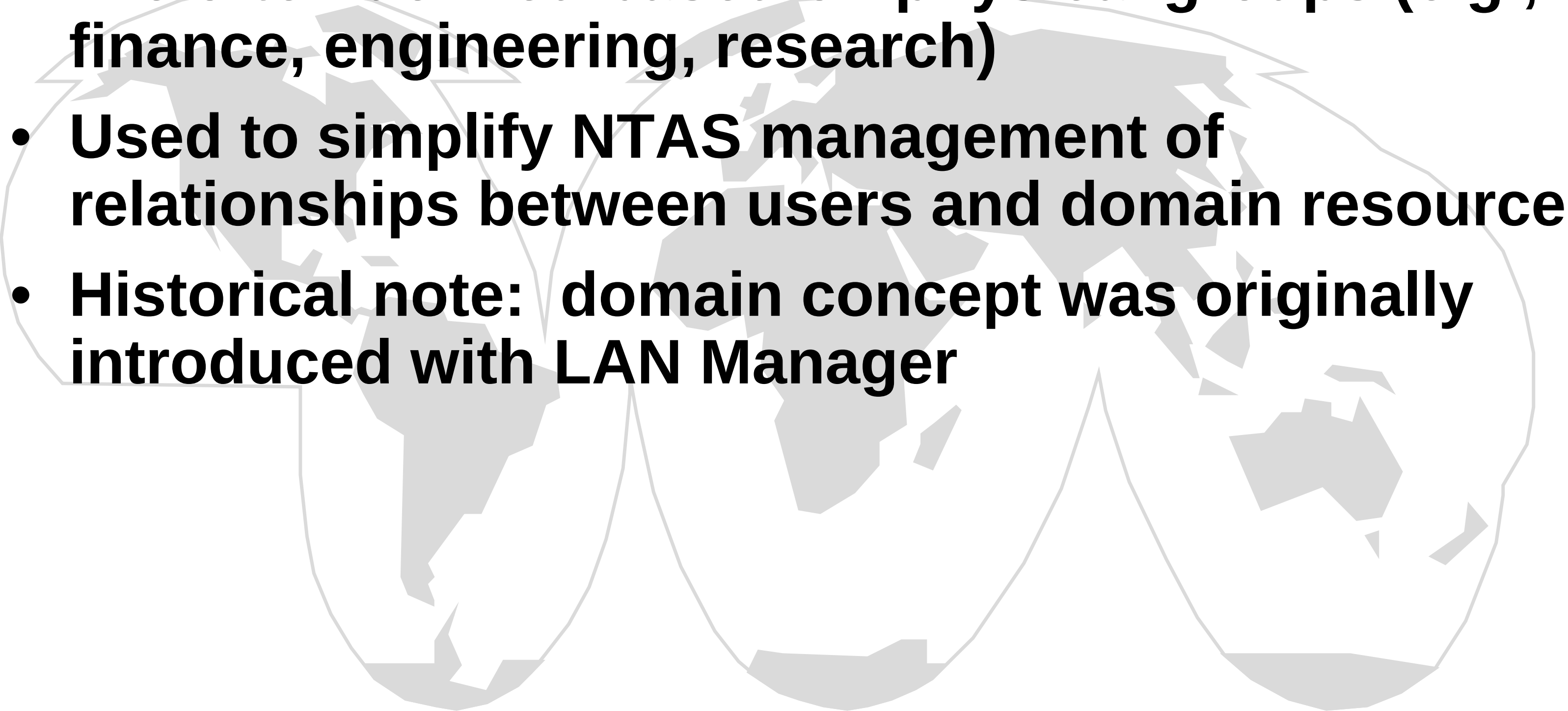
NT Printer Permissions

- Printers may be protected just like other resources
- Local or remote (via peer-to-peer sharing)
- Printers have owners
- Permissions are granted to individual users and groups just like for files and directories
  - No Access
  - Print
  - Manage Documents
  - Full Control

Configuring Permissions

- Limit assignment of “Full Control” permissions
- In general, it is best to start by assigning more stringent permissions--see how they work
- If your NT Advanced Server does not run the NT File System (NTFS), file and directory access is determined by other the mechanisms provided by the other file systems
- Learn more about NT permissions--there are many details and exceptions!

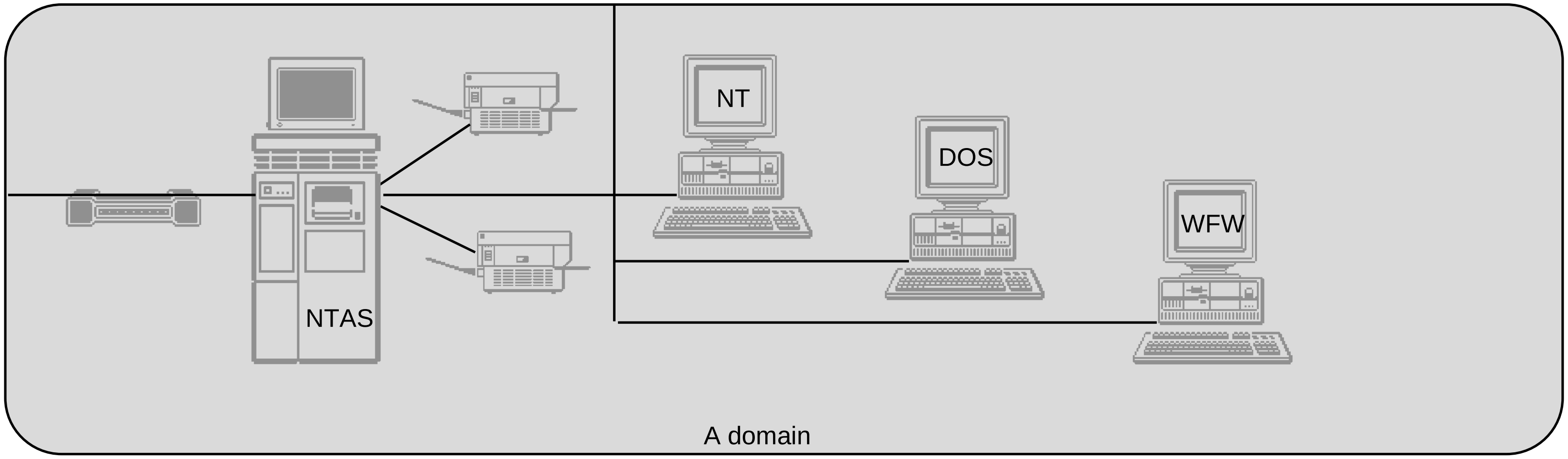
Domains



- **Are often defined based on physical groups (e.g., finance, engineering, research)**
- **Used to simplify NTAS management of relationships between users and domain resources**
- **Historical note: domain concept was originally introduced with LAN Manager**

Domains (continued)

- An NTAS domain consists of
  - One NTAS
  - One or more client PC's
- Domain user accounts can
  - Be members in local and domain-wide groups
  - Only netlogon via the network



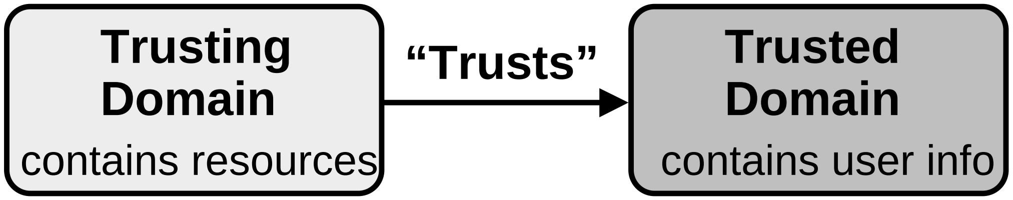
What is Trust?

Trust means all of the following

- Trust is a “one-way street”
- Two trust relationships are required for “two-way street”
- Trust is NOT transitive: A trusts B, B trusts C implies no trust between A and C

Trusting means that your home domain trusts another domain to authenticate a user logging in

Trusted means that your domain contains the database information to authenticate a user



About NT Domains

Why does anyone need domains?

- **Large companies have problems administering all their workgroups individually**
- **Users usually have separate accounts in each domain in which they want to access resources**
- **Sharing resources across several domains is a problem for configuration control**
- **Which domain model you choose depends upon your administration model - centralized or local**

NT addresses these issues using domains, trust relationships, domain accounts, and global groups!

Managing Trust Relationships

Before setting up trust relationships...

Admins need to

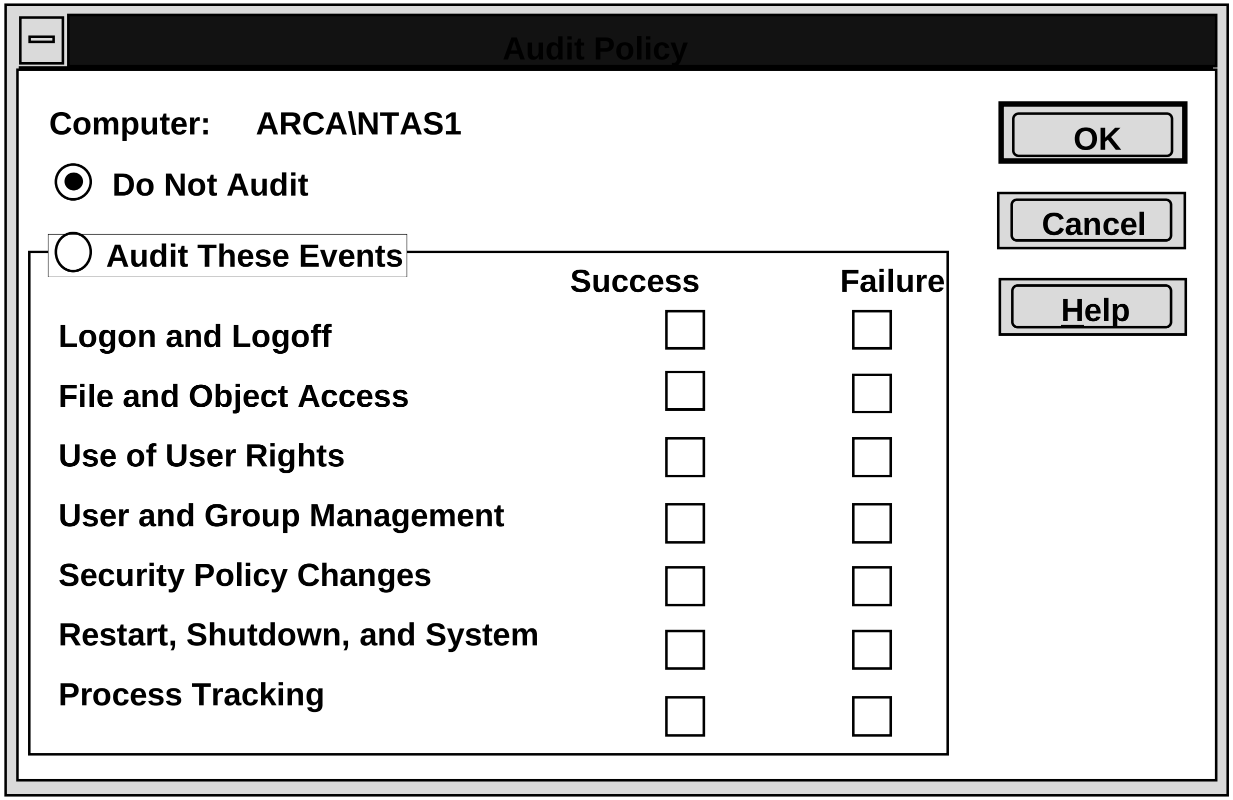
- **determine mutually agreeable naming conventions**
- **know which trust model will be implemented**
- **identify the trust<u>ed</u> and trust<u>ing</u> domain(s)**
- **define directions of trust relationships**
- **select suitable trust relationship passwords**

About NT Auditing

- **Default is *NO* auditing**
  - Each object must be explicitly configured for auditing
  - No user-defineable events
- **NT auditing configuration options include**
  - Auditing policy
  - Audit what resources, which events, and by who
  - Disk space allocation for audit logs
  - What to do if disk space gets filled
- **Four Log types**
  - System
  - Security (audit)
  - Application
  - Performance

Configuring NT Audit Policy

First step - configure NT audit categories (include success/failure of each)



Computer: ARCA\NTAS1

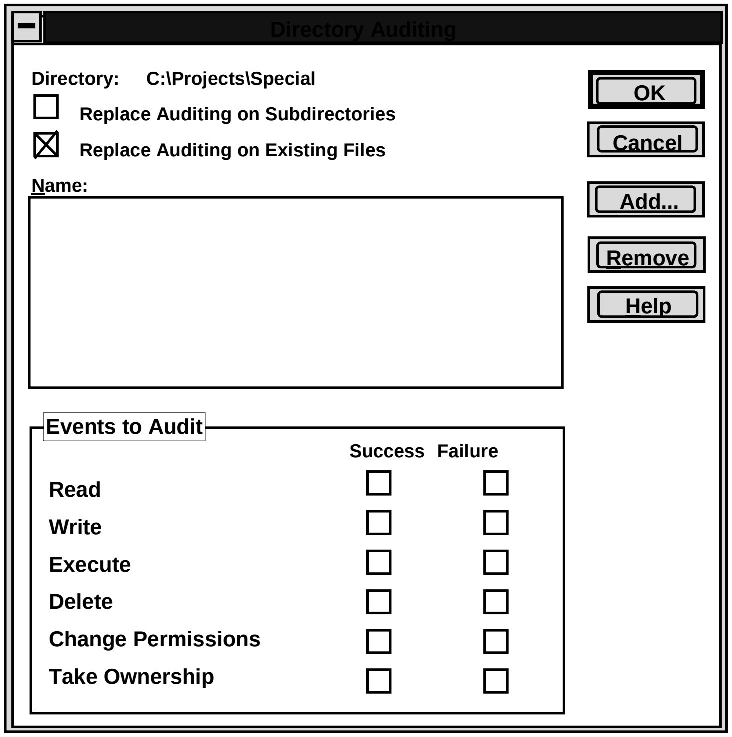
● Do Not Audit

○ Audit These Events

	Success	Failure
Logon and Logoff	□	□
File and Object Access	□	□
Use of User Rights	□	□
User and Group Management	□	□
Security Policy Changes	□	□
Restart, Shutdown, and System	□	□
Process Tracking	□	□

Directory and File Auditing

Next step - designate which directories and files will be audited (applicable only if Audit Policy - File & Object Access category is selected)



Directory: C:\Projects\Special

☐ Replace Auditing on Subdirectories

☒ Replace Auditing on Existing Files

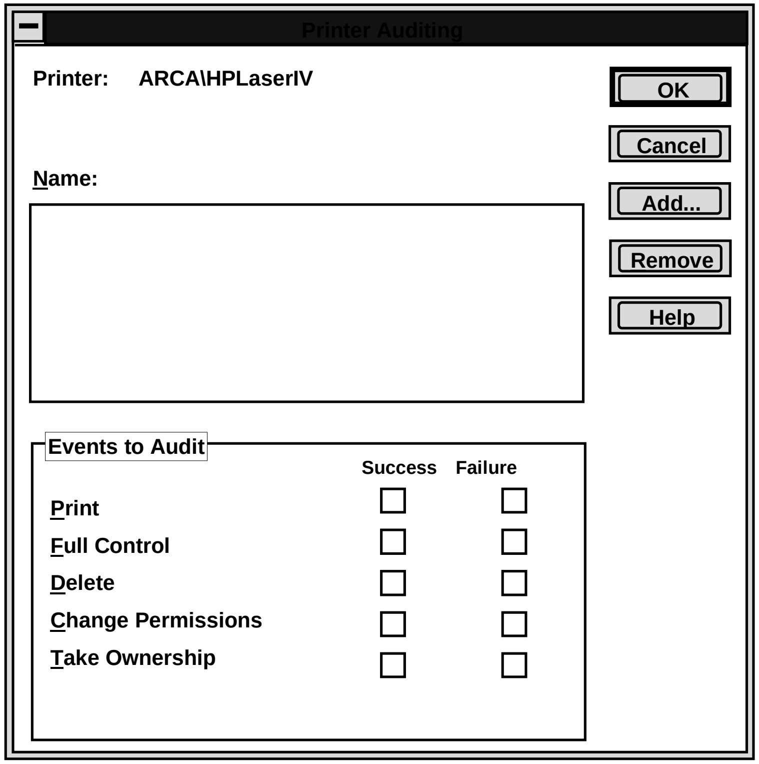
Name:

Events to Audit

	Success	Failure
Read	☐	☐
Write	☐	☐
Execute	☐	☐
Delete	☐	☐
Change Permissions	☐	☐
Take Ownership	☐	☐

Printer Auditing

You can also audit printer usage



Printer: ARCA\HPLaserIV

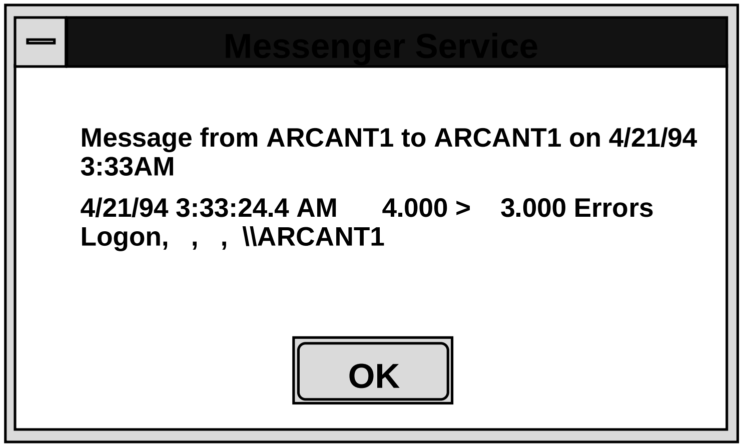
Name:

Events to Audit

	Success	Failure
Print	□	□
Full Control	□	□
Delete	□	□
Change Permissions	□	□
Take Ownership	□	□

NT Administrator Alerts

- Alerts support remote security administration
- Automatic alerts are sent for
  - Security and access problems
  - User session problems
  - Server shutdown when UPS service is available
  - Printer problems
  - Disk problems
- Are configurable



Message from ARCANT1 to ARCANT1 on 4/21/94 3:33AM

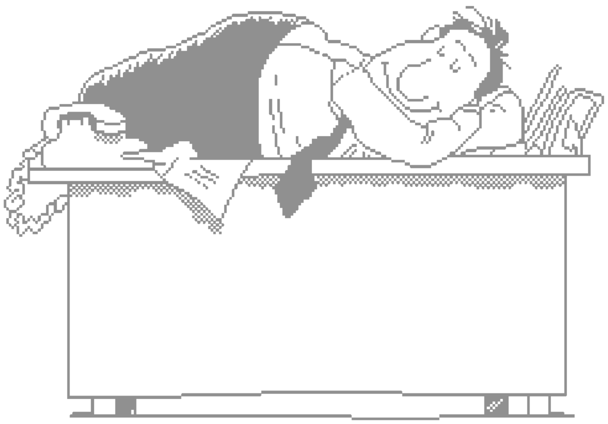
4/21/94 3:33:24.4 AM 4.000 > 3.000 Errors Logon, , , \\ARCANT1

Conclusions about Auditing and Alerts

- NT auditing is good for a LAN, but nevertheless is limited
  - Admin can turn auditing off
  - Audit entries are somewhat cryptic
  - Manual correlation ne cessary to conclude that an intrusion/misuse has occurred
- Adjust the amount of auditing to your security needs
- Alert capability is very useful--use it!
  - You can, for example, compensate for the absence of a badlogon limit by sending Admin an alert after a criterion number of badlogons is reached
  - Be sure that you send the alerts only to the appropriate users

NT Backup

- A subset of Conner Peripherals BackupExec utility
  - Normal Backup
  - Copy Backup
  - Incremental Backup
  - Differential Backup
  - Daily Copy
- Not included are
  - Backup logs
  - Tape cataloging
  - Scheduled, unattended backups
  - Backups of remote Registry files
- *Caution--a Backup Operator making a backup can read and restore all files and directories!*



Viruses and Windows NT

- A virus is a segment of self-replicating code that operates by modifying an application or executable component of a system
- Because NT has memory protection, it is unlikely that a virus could take control of NT’s operating system
- It is possible that a DOS virus could infect a subsystem such as NT’s DOS Virtual Machine, but the capability of such a virus to spread is uncertain
- There are currently no viruses that target NT
- The threat of virus infections in NT is currently overshadowed by a number of larger security concerns!

NT Information on the Internet

- Newsgroups
  - comp.os.ms-windows.nt.misc

    covers all topics related to Windows NT
  - comp.os.ms-windows.nt.setup

    covers installation and configuration questions

- FTP
  - ftp.microsoft.com

    new drivers, patches, tools, unsupported, etc...

Final Conclusions

- NT Advanced Server is a BIG step forward for workstation and server security
  - Many security features
  - Even more in NT Advanced Server
- Security must be planned and configured
  - Set policy
  - Implement with NT and procedures
  - Configure system to support policy
- NT Client and NT Advanced Server
  - Requires planning and work to secure
  - Lots to learn