Microsoft® Windows NT® Server:

Security Features and Future Direction

White Paper

Coopers & Lybrand L.L.P.
Information Technology Security Services

C

About Coopers & Lybrand

Coopers & Lybrand L.L.P. is one of the world's leading professional services firms providing audit, tax, management consulting, financial advisory, and human resource advisory services to clients in a broad range of industries on a globally integrated basis in 140 countries. In the United States, the firm has been serving clients since 1898 and today has 17,000 partners and staff working in over 100 offices. Organized along industry lines, the firm seeks to create value for its clients and to bring a competitive advantage to their activities. Its clients include a variety of large and small, publicly and privately held companies, many numbered among the Fortune 500.

Coopers & Lybrand L.L.P. has recognized the risks and threats to information since the early stages of information technology development. Their original approach to auditing computer based systems included the study and evaluation of controls over the security of information. The firm has since established the Information Technology Security Services (ITSS) national practice dedicated to serving their clients' needs in addressing security over one of their most important resources--technology generated and resident information. The ITSS professionals are recognized leaders in the fields of information technology, telecommunications, logical and physical security, and auditing. They are knowledgeable in the latest security tools and methods, and in reviewing, analyzing, developing and implementing security and control solutions.

Services offered by the ITSS practice include Electronic Commerce Security Implementation and Assessment, Enterprise Security Assessment, Penetration Testing, Internet Connectivity Reviews, Firewall Reviews, Operating System Security Reviews, Information Security Risk Analysis, Security Plan Development, Policy and Procedure Development, Business Continuity Planning Review, and Training.

About The Authors

Trevor Boll is a Senior Associate in Cooper & Lybrand's Information Technology Security Services (ITSS) practice. He has performed enterprise-wide security reviews over multiple networks and operating systems for numerous clients. Trevor's technical focus is in Windows NT, NetWare, and Internet security. Trevor earned an M.B.A. from the University of Utah and a B.S. in Finance from Brigham Young University..

Paula Chamoun is a Senior Associate in the Computer Assurance Services (CAS) group of Coopers & Lybrand L.L.P. Her background includes Novell Networks, developing applications using genetic algorithms and neural networks, and programming in C, C++, Oracle, and Powerbuilder. At Coopers she has performed an extensive array of IT assurance services for large financial services and manufacturing clients. Paula is a member of ISACA and is a Certified Information Systems Auditor. She earned an M. S. in Management Information Systems from the University of Virginia and a B. S. in Computer Science from Pace University.

David Cohen is a Manager in Coopers and Lybrand's ITSS practice based in New York City. David is a manager in the ITSS group. He oversees the Electronic Commerce and Cryptography services in the NY office. His roles and responsibilities also include managing consultations related to the controls over UNIX and Windows NT system and application security, the UNIX operating system, and Internet and private networking environments. David has B. S. in Statistics from Cornell University.

Neil Cooper is a Senior Technical Manager of Coopers & Lybrand's Information Technology Security Services (ITSS) practice, and has over 16 years experience in data processing. Neil has primary responsibility for leading the Windows NT security service line for Coopers & Lybrand and is part of Coopers & Lybrand's technical team for UNIX, Windows NT, NetWare, and Internet Security Services. Neil's technical capabilities include knowledge of UNIX, TCP/IP, X-Windows, as well as mid-range systems. Neil earned an M. S. in Geology from the University of Delaware and a B.S. in Geology from Pennsylvania State University.

James Jumes is a Senior Manager of Coopers & Lybrand's Business Systems Advisory Services (BSAS) and Security practices, and has over ten years of information technology strategy, business system selection and implementation, and security experience. James is one of the principal authors of the book, *Windows NT 3.5 Guidelines for Security, Audit, and Control*, and has developed a Windows NT 3.5x security review program and recommendations tool. James earned an M.B.A. from Lehigh University, and an M.Ed. and B.A. in Psychology from Boston College.

Mark Lobel is a Technical Manager in Cooper's & Lybrand's Information Technology Security Services (ITSS) practice. Mark's technical focus is on Windows NT and a variety of UNIX flavors including AIX, Solaris, Digital UNIX, HP-UX, FreeBSD, Linux, and DG-UX, Internet security (Firewalls, topologies, protection strategies), TCP/IP networking, remote access connectivity, and data encryption assessments. He has also served as a system administrator for a Novell and UNIX based systems and taught UNIX and Internet usage at Boston University. Mark earned his MBA from Boston University and a BA in Broadcast Communications from Oswego State and is designated a Certified Information Systems Auditor (CISA).

Paul Olson is a Senior Consultant in Coopers & Lybrand's Business Systems Advisory Services (BSAS) practice in San Francisco. Paul's technical focus is on PC, LAN, and UNIX platforms. Paul earned a B. S. in Management Information Systems and Accounting from the California Polytechnic State University at San Luis Obispo.

Bruce Murphy is the National Partner of Coopers & Lybrand's Information Technology Security Services (ITSS) practice based out of the New York region. He has over eleven years of experience implementing access control mechanisms, from a management, technical, and procedural perspective, across PC, LAN, mid-range, and mainframe computing platforms. Bruce lectures frequently on many areas of information security, including Electronic Commerce, Multi-Platform Network Architectures, Local Area Networks, Toll Fraud, and Advanced Authentication Techniques. Bruce is President of the New Jersey ISSA chapter, and is designated a Certified Information Systems Security Professional. He earned a B.A. in English from Muhlenberg College.

Kevin Reardon is a Senior Technical Specialist in Coopers and Lybrand’s Information Technology Security Services (ITSS) practice based in Washington, DC. Kevin's technical focus is on a variety of UNIX variants (SunOS, IBM AIX, Linux, HP-UX), Windows NT, Internet security (Firewalls, topologies, protection strategies), Novell NetWare, TCP/IP networking, remote access connectivity, and security awareness training. In this capacity he has reviewed system configurations, network topologies, network access points, and assessed the appropriateness of the related security controls. Kevin earned a B. S. in Computer Information Systems from the University of Scranton.

David Rivera is a Senior Technical Manager of Coopers & Lybrand Information Technology Security Services (ITSS) practice, and has over 19 years experience in data processing. David leads Coopers & Lybrand’s technical team for Internet and UNIX Security Services. David's technical capabilities include internal's knowledge of UNIX, TCP/IP, and all Internet protocols and services. David also successfully leads focused Internet penetration exercises from Coopers & Lybrand’s Internet testing lab in New York. David earned an M.S. in Computer Science, and a B.S. in Computer Technology; from the New York Institute of Technology.

Table of Contents

ABOUT COOPERS & LYBRAND 2
ABOUT THE AUTHORS 3

TABLE OF CONTENTS 5

EXECUTIVE SUMMARY 7

SECURITY BASICS 8

CORPORATE IT OBJECTIVES 8
Information Security Requirements 9
IT Security Control Objectives 10

THE EVOLUTION OF WINDOWS NT SERVER 12

SECURITY ARCHITECTURE 14

DESIGN 14
Security Reference Monitor 15
Local Security Authority 16
Security Account Manager 16
Logon Process 16
Discretionary Access Controls 18
Access Control Lists 18
Access Tokens and Security Identifiers (SID) 21
ACCESS CONTROL 22
Introduction 22
User Authentication 22
Windows NT Domains and Trust Relationships 24
Supported Network Transport Protocols 27
SECURITY CERTIFICATIONS 28
C2 - FC2/E3 29
WINDOWS NT SERVER ATTACKS AND DEFENSES 31

SERVICES THAT ENHANCE OR IMPACT SECURITY 35

IMPACT OF THE INTERNET ON SECURITY 35
INTERNET INFORMATION SERVER 35
PROXY SERVER 35
SECURE SOCKETS LAYER (SSL) 36
SERVER-BASED ROUTING 36
POINT-TO-POINT TUNNELING PROTOCOL (PPTP) 37

WINDOWS NT SERVER SECURITY FEATURES 38

DEFINING SECURITY SETTINGS 45
Account Policies 45
User Accounts 46
User Rights 47
Registry Permissions 48
Securing the Registry 48

SYSTEM ENHANCEMENTS THAT AFFECT SECURITY 51

SECURITY FEATURES ADDED SINCE VERSION 3.51 ... 51
CryptoAPI (CAPI) ... *51*
Network Monitor ... *51*
System Policy and User Profiles ... *51*
Task Manager ... *51*
Improved Windows NT Diagnostic Tool ... *52*
Communications Features ... *52*
Internet ... *52*
Remote Registry Access ... *53*
Default Settings ... *53*
FTP Service Directory ... *53*
WINDOWS NT 4.0 SERVICE PACK 3 ... 53
SMB Signing ... *53*
Using a System Key to Strongly Encrypt Password Information ... *54*
Password Filtering ... *54*
Restricting Anonymous User Access ... *55*
CryptoAPI 2.0 ... *55*
TCP/IP Improvements to resist OOB Denial of Service Attacks ... *55*

FUTURE DIRECTION: WINDOWS NT 5.0 ... 57

CONCLUSION ... 59

APPENDIX 1: SECURITY AWARENESS ... 60

INTRODUCTION ... 60
THE IMPORTANCE OF AWARENESS ... 60
THE PHYSICAL FACTS ... 61

BIBLIOGRAPHY ... 62

FIGURE 1: WINDOWS NT SERVER ARCHITECTURE (SCHEMATIC) ... 15
FIGURE 2: WINDOWS NT LOGON PROCESS ... 18
FIGURE 3: OBJECT SECURITY DESCRIPTOR ... 21
FIGURE 4: SINGLE DOMAIN MODEL ... 25
FIGURE 5: MASTER DOMAIN MODEL ... 26
FIGURE 6: MULTIPLE MASTER DOMAIN MODEL ... 26
FIGURE 7: COMPLETE TRUST MODEL ... 27

TABLE 1: IT OBJECTIVE COMPONENTS ... 9
TABLE 2: IT SECURITY CONTROL OBJECTIVES ... 11
TABLE 3: STANDARD PERMISSIONS FOR ACL'S ... 21
TABLE 4: WINDOWS NT ATTACKS AND DEFENSES ... 34
TABLE 5: WINDOWS NT SECURITY FEATURES ... 45
TABLE 6: ACCOUNT POLICY ... 46
TABLE 7: REGISTRY SUBKEY PERMISSIONS ... 49
TABLE 8: REGISTRY ROOT KEY PERMISSIONS ... 50

Executive Summary

The objective of this paper is to document the security architecture and features of the Windows NT Server Operating System, striking a balance between general security issues and a more technical perspective.

Microsoft's Windows NT Server operating system is a general purpose operating system. It supports application oriented services,such as databases and web servers, as well as Network Operating System (NOS) type services such as print and file services. The Windows NT Server operating system release that is current at the time of the creation of this document is Windows NT Server version 4.0 with Service Pack 3[1] (SP3) applied. This document is written in the context of that configuration, with a section noting significant changes and enhancements since version 3.51, the previous major release.

Microsoft's stated design and market goals for the Window NT Server operating system, as conveyed to Coopers and Lybrand LLP, are to provide a platform which is broadly useful for business and government computing including, but not limited to, on-line transaction processing, large-scale data management, Internet services including Electronic commerce, decision support computing including data warehousing and enterprise groupware/messaging systems. Windows NT Server is supported on a wide range of hardware from small, single disk uniprocessor systems to very large, symmetric multiprocessor (SMP) data center systems, from many hardware companies. In addition to large, single servers, the "domain" structure of typical Windows NT-based networks often includes several servers sharing a common logon, and providing services to a single user base.

In May 1997, Microsoft announced a high-end variant of the Windows NT Server, called Windows NT Server Enterprise Edition, including scalability and availability enhancements. This release is currently in beta release testing; as it is based on Windows NT Server version 4.0 SP3, its security will not be discussed separately.

To be consistent with the goals stated above, an operating system needs to have a significant focus on security. Not only must the operating system provide for core security functions such as authentication, granular access control, process isolation, confidential wide-area communications, and audit trails, but the security architecture must be scaleable and extensible. It must be scaleable, so that large servers and large networks can authenticate large numbers of clients and objects, without excessive performance overhead. It must be extensible to allow for new technologies to be added, such as smart cards, as these technologies comes into common use.

When properly installed and deployed, and when managed by competent system management personnel who are under appropriate supervision, Windows NT Server version 4.0 SP3 appears to provide the range of features and capabilities necessary to support a wide range of business and government tasks in a secure, reliable fashion.

[1] Service Pack - a maintenance release of the software, used to correct problems and make changes.

Security Basics

Security: What is it?

Security is a term with both a business meaning and a technical meaning. In this paper we will discuss the issue on both levels, and discuss the relationship between technology and business process where appropriate. Security depends, however, on more than just technology. It depends on the proper administration of systems, client and server, as well as the faithful observance of related business procedures, physical access controls, and audit functions.

As a business matter, security usually means:

- Legitimate use
- Confidentiality
- Data integrity
- Auditablility

Looking at each of these, legitimate use requires the authentication of users. It requires granular controls over which users can access what data, and execute which programs. Confidentiality implies that a system will provide appropriate services, such as data encryption, to ensure that only authorized personnel can see sensitive data. Data integrity requires a robust file system, and ways for files or databases hosted on the operating system to recover from system, application and network faults and failures. Auditablility requires that systems have the ability to log a wide variety of events for review, that these log files are themselves secure, that actions (“alerts”) can be triggered by certain events which may indicate that a system, account or application is under attack.

Security is not absolute -- there is not one standard that will fit all businesses and industries. National defense applications, or funds transfer in a financial institution, will require a more secure system than order entry in a small business, for example. While Windows NT Server provides a wide range of features and settings, individual enterprises and government accounts will need to carefully assess their security needs and make appropriate security decisions about standard and/or optional security products.

Corporate IT Objectives

The general requirements of Information Technology necessary for a corporation to effectively meet its business objectives may be stated as the Corporate IT Objectives. By varying the degree of emphasis it places on each of these requirements and adding in user needs and regulatory requirements, a corporation can tailor the following general IT objectives into its own unique Corporate IT Objectives. Once formulated, these Corporate IT Objectives will constitute the goals of a corporation's information technology systems strategy. The general components of these objectives are described in Table 1 that follows:

Objective	**Description**
Effectiveness	Deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner.
Efficiency	Concerns the provision of information through the optimal (most productive and economical) use of resources.
Compliance	Deals with complying with those laws, regulations and contractual arrangements to which the business process is subject, i.e., externally imposed business criteria.
Reliability of Information	Relates to the provision of complete and accurate information for management to operate the entity and for management to exercise its financial and compliance reporting responsibilities.
Confidentiality	Concerns the protection of sensitive information from unauthorized disclosure.
Integrity	Relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations.
Availability	Relates to information being available when required by the business process now and in the future; it also concerns safeguarding of necessary resources and associated capability.

Table 1: IT Objective Components

Information Security Requirements

Of the general requirements for information technology to effectively meet its business objectives, the following three are necessary for effective security: Confidentiality, Integrity, and Availability. Depending on a Corporation's IT and Business Objectives, the emphasis of each security requirement differs. For example, a highly sensitive system, such as a national defense system, has a greater need for confidentiality of classified information, while an electronic funds transfer system or a medical system has a greater need for strong integrity controls and an automated teller machine has a greater need for all three.

Confidentiality

Protecting information from unauthorized disclosure. The system should be designed and implemented to ensure the optimum control over computer data and program files. Privacy, sensitivity, and secrecy are issues here.

Integrity

Provide adequate protection from unauthorized, unanticipated or unintentional modification ensuring data is accurate and complete, including:

1) Ensuring consistency of data values within a computer system;
2) Recovering to a known consistent state in the event of a system failure;
3) Ensuring that data is modified only in authorized ways;
4) Maintaining consistency between information internal to the computer system and the realities of the outside world.

Availability

Information must be available on a timely basis wherever it is needed to meet business requirements or to avoid substantial losses. Uninterrupted access to information and system resources, such as data, program and equipment, is a fundamental need.

IT Security Control Objectives

The IT Security Control Objectives are the desired security goals to be achieved by implementing IT security controls. The achievement of these goals will help a corporation meet its overall IT Control Objectives and satisfy the security requirements of its information. These objectives are detailed in Table 2 below:

Security Objective	**Description**
Security monitoring	Management should monitor whether a secure computer environment is maintained.
Security management	Management should ensure the implementation of access control policies, which are based on the level of risk arising from access to programs and data.
System level access controls	Access to the computer system, programs, and data should be appropriately restricted.
Application level access controls	Access to particular functions within applications (e.g., approving payment of vendors) should be appropriately restricted to ensure segregation of duties and prevent unauthorized activity. (Where applications do not provide access control facilities, this objective should be addressed by

Security Objective	**Description**
	system level controls.)
Sensitive facilities	Use of sensitive facilities, such as master passwords, powerful utilities, and system manager facilities, should be adequately controlled.
Physical access	Physical access to computer facilities and data should be appropriately restricted.
External network connections	External network connections should be used for valid business purposes only and controls should be in place to prevent these connections from undermining system security.

Table 2: IT Security Control Objectives

The above described security control objectives may be applied in the Windows NT environment by following the model that is explained in the following sections, which explain the architecture and the features of Windows NT security and how they operate within the constraints of the operating system.

The Evolution of Windows NT Server

The most notable design objectives for Windows NT were and still are:

- **Extensibility** The ability for the Windows NT operating system to grow over time and meet market requirements. Extensibility maybe accomplished through Windows NT's modular design, the creation of a privileged processor mode (kernel mode) and nonprivileged processor mode (user mode), use of objects, ability to load device drivers, remote procedure call facility, and the ability for applications to utilize the Windows NT services.
- **Security** The role of security in an operating system was analyzed and the layered security model of Windows NT resulted. This was accomplished through the development of the Security subsystem and its associated components: LSA, SRM, SAM, and the discretionary access controls.
- **Portability** The ability to function on multiple architectures. Windows NT may operate in certain CISC and RISC architectural environments. Portability may be accomplished through the Windows NT Hardware Abstraction Layer. This layer separates Windows NT from the architecture.
- **Reliability** The ability to guard against adverse potential events; robustness. Reliability , was designed into NT through its government C2 security rating and the error exception handling capability.
- **Compatibility** The ability to execute applications written for other operating systems. Windows NT can run the 32 bit applications, MS-DOS 16-bit applications, as well as certain OS/2 applications and POSIX applications.
- **Performance** The ability to process data calculations rapidly. Performance goals may be accomplished through Windows NT's ability to utilize faster multiprocessors, multiple processors (SMP), memory management, and optimized system services.

Windows NT Server version 3.1 was released in June 1993. This first version of the operating system gained some market acceptance in the low-mid range application server market and the network operating system market. Version 3.5 SP3 received its C2 Orange Book rating (see page 29) in August 1995 and version 3.51 received F-C2/E3 certification in October 1996. Security has been enhanced in the release (version 4.0) since version 3.51 and these are discussed on page 51 in the section entitled Security Features Added since version 3.51. Windows NT Server version 4.0 SP3 is the current release, its new or additional security features are documented starting on page 53.

The next release of Windows NT, V5.0, is expected to become a beta product in 1997 and will have some additional security features. These features, to the extent that information is currently available, are described in Future Direction: Windows NT 5.0 on page 57.

With the changes that Microsoft has made to Windwos NT since its initial release, Windows NT Server is now used across a variety of applications, even in demanding production environments such as SAP R/3.

Security Architecture

Design

Windows NT Server utilizes an integrated architecture to authenticate, validate and record information about security within the operating system. The security architecture consists of several components:

- Security Reference Monitor
- Local Security Authority
- Security Account Manager
- Mandatory, Secure Logon Process
- Discretionary Access Controls
- Access Tokens and Security Identifiers
- Access Control Lists

The overall system architecture is divided into two main areas: the kernel and user. These are shown in the diagram, Figure 1: Windows NT Server Architecture (Schematic), on page 15. The segments of the architecture that relate to security: Security Reference Monitor, Security Subsystem and the Logon Process; are highlighted on the diagram. Within this architecture, Windows NT is able to apply security to every object and process it controls. This means that every object resident on the Windows NT computer and every process running on that computer are subject to the security controls of the overall architecture.

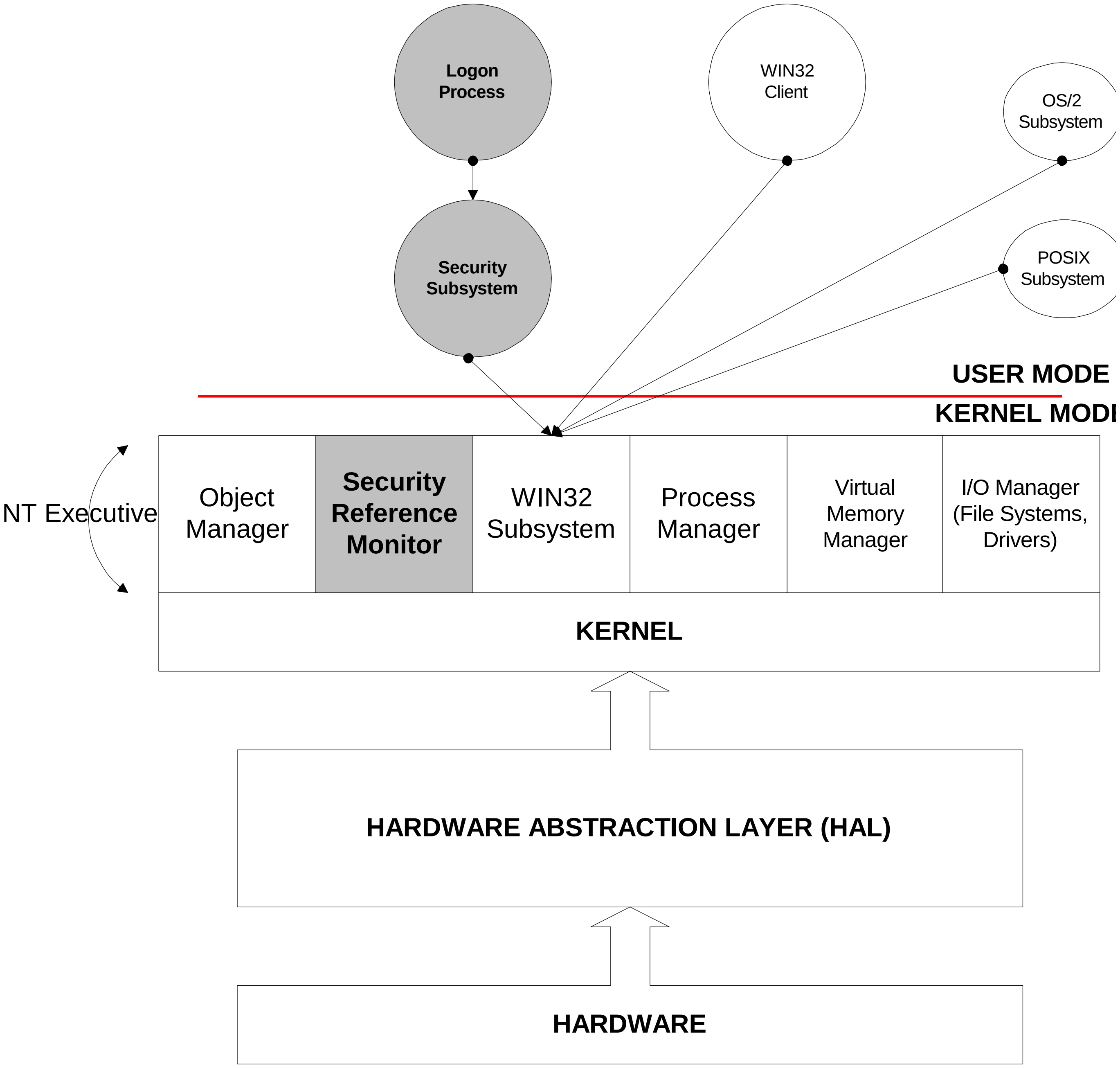

Figure 1: Windows NT Server Architecture (Schematic)

Security Reference Monitor

The Security Reference Monitor (SRM) is part of the NT Executive within the NT Kernel as shown in Figure 1 on Page 15, with the security functions highlighted in gray. It is responsible for enforcing all access validation and audit policies defined within the Local Security Authority. In this way, the SRM is designed to protect all system objects from unauthorized access or modification. The SRM is the repository for the system's access validation code and is the only copy of that code on any given Windows NT system. This ensures that all protection is provided uniformly to objects on the system. The SRM provides services for validating access to objects, generating audit messages that are subsequently logged by the Local Security Authority, and verifying user accounts for the appropriate privileges.

Local Security Authority

The Local Security Authority (LSA) provides many services to the security subsystem of the Windows NT operating system. It is designed to ensure that the user has permission to access the system by validating the users logon. It manages the local security policy as set by the administrator, it generates access tokens, and provides interactive validation services when access is requested for any system object. The LSA also controls the audit policy, set by the administrator, and writes any messages generated by the Security Reference Monitor to the event logs.

Security Account Manager

The Security Account Manager (SAM) controls and maintains the Security Account Database (SAD). The SAD is part of the registry and is invisible to the users during normal processing. The SAD contains account information for all user and group accounts. The SAM provides the user validation service during logon that is used by the LSA. It compares the cryptographic hash of the password given at logon time with the hashed password stored in the SAD. It will then provide the user's Security Identifier (SID), as well as the SIDs for any group the user belongs to, back to the LSA for the creation of the access token that will be used during that session.

Logon Process

The Windows NT logon process, which is diagrammed in Figure 2 on Page 18, is mandatory for initiating a session with a Windows NT server or workstation. The logon process differs slightly if the user is attempting to logon to a local machine or to a remote server in a network. The logon is a multi-step process that follows part A or part B of the following list. The numbers that follow the steps match the step with pictures included in Figure 2.

A) Local Machine Logon

- Press ctrl+alt+delete keys together to display a logon dialog box (1)
- Type the userid and password (1)
- Press enter
- The password is hashed and sent to the local Local Security Authority (LSA) (2,3)
- The LSA makes a call to the MSV1_0 authentication package and compares the hash to the hash stored in the local SAM database (4,5)
- The LSA creates an access token using the user's account SID and group SIDs returned from the MSV1_0 authentication package (6,7)
- The NT Explorer Shell opens with the user's access token attached (8,9)

B) Domain Account Logon

- Press ctrl+alt+delete keys together to display a logon dialog box (1)

- Type the userid, password, and select the domain (1)
- Press enter
- The password is hashed and sent to the local Local Security Authority (LSA) (2,3)
- The LSA makes a call to the MSV1_0 authentication package
- Because the account does not come from the local account database, MSV1_0 calls the NETLOGON service to establish a secure RPC session with a domain controller for authentication
    - The server issues a 16 byte challenge packet called a nonce[2] (2,3)
    - The nonce and the hashed password are encrypted together (3)
    - This encrypted response is sent back to the server (3)
    - The server uses the nonce plus the hashed password from its SAM to create a copy of the response (4,5)
    - The response from the user is compared to the server's created response (5)
- The NETLOGON service on the domain controller passes the information to the MSV1_0 authentication module on the domain controller, which is in turn compared to the SAM database (4,5)
- The NETLOGON service on the domain controller returns the user’s SID and global SID information to the requesting client
- NETLOGON on the client returns the SID information obtained from the domain controller to the local LSA process
- The local LSA process looks in the local SAM database to acquire local group SID information
- The user SID, global SID, and local SID information is used generate the access token (6,7)
- Explorer Shell opened with the user’s access token attached (8,9)

[2] nonce: a one-time randomly generated number.

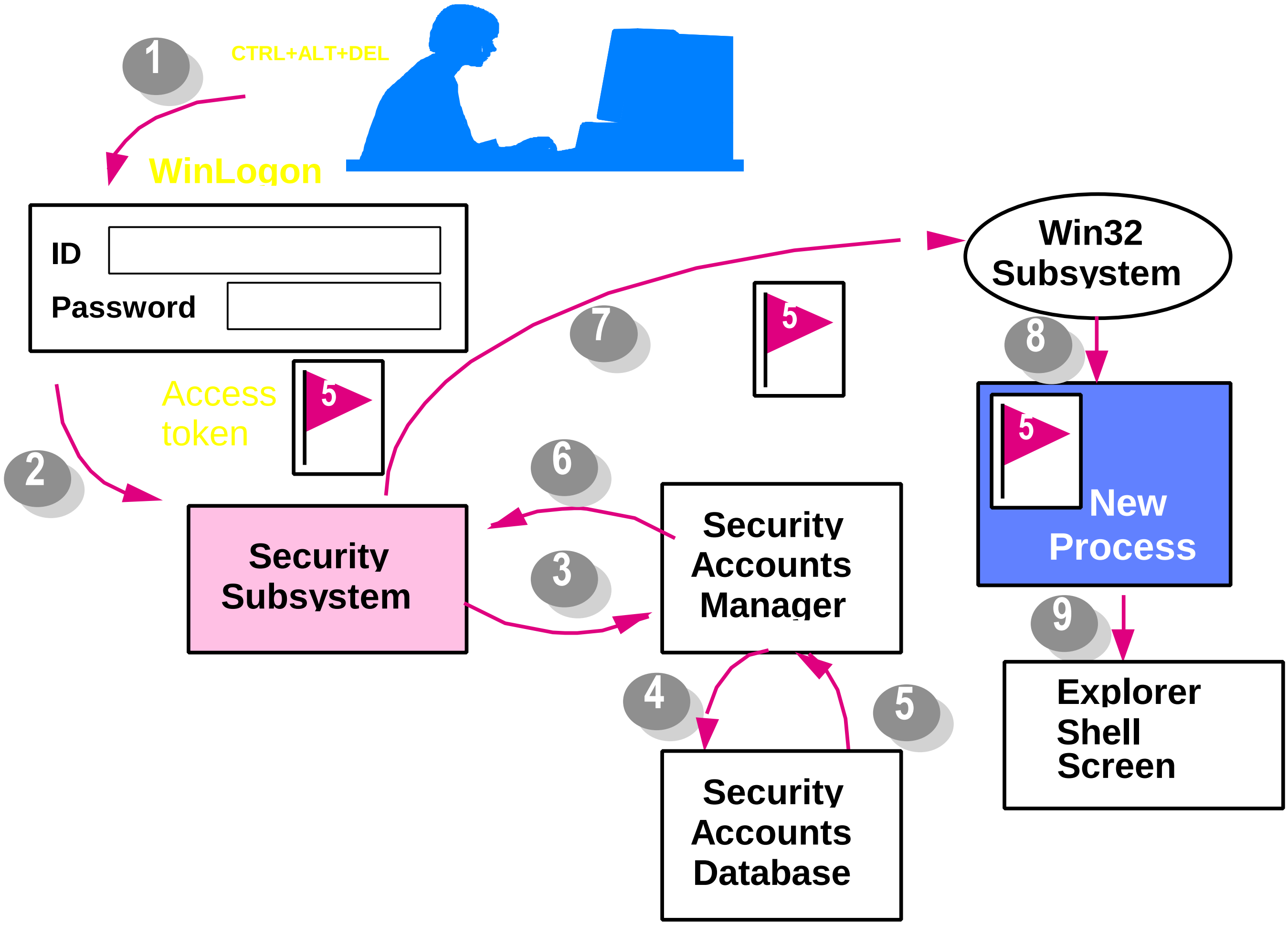

Figure 2: Windows NT Logon Process

Discretionary Access Controls

Discretionary Access Controls (DAC) provide object and resource owners the means to control who can access resources as well as how much access they may have. Access to system resources, such as files, directories and folders, printers, network shares, and system services, can be controlled either through GUI-based system tools or through the command line.

Objects in Windows NT support discretionary access controls. The NT Explorer, Print Manager, User Manager for Domains, and Server Manager are tools used to manipulate DACs on the common objects that users and administrators work with in the Windows NT environment.

Access Control Lists

Objects within a Windows NT system may have an Access Control List. Access Control Lists

(ACL) are lists of users and groups that have some level of permissions to access or operate an object. Each object in the Windows NT system contains a security descriptor, shown in Figure 3 on page 21, which is comprised of the Security Identifier of the person who owns the object, the regular ACL for access permissions, the system ACL (SACL) which is used for auditing, and a group security identifier.

ACLs may be composed of Access Control Entries (ACE). There are situations where an ACL will have no ACEs. This is known as a null or empty ACL. Each ACE describes the permissions for each user or group that has access to an object. Access Control Entries within Windows NT are composed of permission categories known as either standard or special. Each permission type is valid for both files and directories. Special permissions consist of the six individual permissions, while the Standard permissions are combinations derived from the special permissions. These permission levels include No Access, a level of authority that may supersede all other authorities.

An example of the No Access permission may be described in this manner:

- The local group named Marketing is granted read access to files in a directory called data.
- The Domain User named joseph, a member of Marketing, is specifically listed as No Access to the data directory.
- Therefore, joseph is not able to read the files in the data directory, while all other members of Marketing may.

The permissions described in the following list and in Table 3 may be characterized as NTFS ACL permissions.

The special permissions include:

- R - Directory: permitted to view names of files and subdirectories
  - Files: permitted to read file's data

- W - Directory: permitted to add files and create subdirectories
  - Files: permit changing of file data

- X - Directory: permitted to change to subdirectories (cd)
  - Files: permitted to run file if it is a program

- D - Directory: permitted to delete directory and subdirectories
  - Files: permitted to delete files

- P - Directory: permitted to change directory permissions
  - Files: permitted to change file permissions

- O - Directory: permitted to take ownership of directories
  - Files: permitted to take ownership of files

The standard permissions include:

Permission Name	**Directory Permission**	**File Permission**	**Explanation**
No Access	None	None	No access to files and directories
List	RX	Not Specified	List Directory Contents Change to subdirectories No access to files unless granted explicitly
Read	RX	RX	List Directory Contents Change to subdirectories Read data from files Execute programs
Add	WX	Not Specified	Create subdirectories Create files No access to existing files unless granted explicitly
Add & Read	RWX	RX	List Directory Contents Change to subdirectories Create subdirectories Read data from files Execute programs
Change	RWXD	RWXD	List Directory Contents Change to subdirectories Delete subdirectories Create subdirectories Read data from files Create and modify files Execute programs Delete files
Full Control	All	All	All directory permissions

Permission Name	Directory Permission	File Permission	Explanation
			All file permissions Change permissions Take ownership

Table 3: Standard Permissions for ACL's

There are other forms of ACLs in a Windows NT system. These include registry permission ACL's which contain two standard permissions and one special permission which contains 9 subpermissions for manipulating registry keys. The registry subpermissions are described in Table 7 on page 49. Another type of ACL is the printer ACL, for managing printers and documents.

Error! No topic specified.

Figure 3: Object Security Descriptor

Access Tokens and Security Identifiers (SID)

Access tokens are created, by the Local Security Authority after SAM validation, as part of a successful logon process. The access token created at that time stays with that particular user's session for as long as they stay logged on. Whenever a user initiates a process during the course of the session, a copy of the token is attached to that process. Once the user logs off, the token is destroyed and will never be used again. Each token contains the following information:

- User's Security Identifier (SID)
- Group Security Identifiers
- User privileges
- Owner (SID assigned to any objects created during the session)
- Primary Group SID
- Default ACL (assigned to any object created by the user)

Access Control

Introduction

Windows NT provides security features in the area of access control. Chief among them is the NT File System (NTFS). NTFS is one of the two file system technologies supported under Windows NT, but it is the only Windows NT-based file system to provide security functionality at the file and directory level. In addition to providing physical security for a Windows NT Server, which is critical, the implementation of NTFS is the only file system that should be utilized if you want to deploy a secure environment.

NTFS is a file system that treats each file and folder as an object. Each object contains attributes, stored with the object, such as size, name, and security descriptor. The file system itself contains a Master File Table that keeps track of the information stored on the file system, as well as the information needed to perform a file or directory recovery.

Windows NT provides for granular access control. As is noted in the section entitled Security Certifications on page 28, the basic system design was created with the requirement of discretionary control in mind, as described in the US government's 'C2' specification. This means the operating system must allow the owner of any object the ability to permit or deny access to that object. Objects include programs, files, directories, processes, printers, etc. Windows NT accomplishes this level of control through the use of Access Control Lists. When a user executes the logon process, an access token with all the users' rights (name of the authenticated user, any groups the user is assigned to, etc.) is created and follows the user throughout the session. This token is applied to any processes started by the user so the process will have the same rights as the user (inherited token). If the user (or group the user is assigned to) is defined as the owner of an object, or part of a group allowed to access an object (as defined in the ACL), access is granted. In all other cases, access is denied. Additionally, in the access control list, a system administrator, or owner of an object, can define what type of access is allowed to the object. These levels of access include Full Control, Change, Read, Write, Execute, Delete, Change Permissions, Take Ownership, and No Access.

In addition to the ACL concept, there are additional levels of control. There are 27 specific 'user rights' that can be assigned (or restricted) to users or groups in Windows NT. These levels include the ability to access a computer from the network, to change the system time, to log onto the system locally, the ability to take ownership of objects, and even to shut down the system. Finally there are specific account restrictions that can be placed on an account to control the users access to the system. These include password restrictions, logon times, remote access capabilities, group memberships, intruder detection/account lockout, and user specific profiles.

User Authentication

User authentication, determining a user's identity, is the foundation for Windows NT security.

Successful authentication will facilitate access to authorized resources. Unauthorized users that can masquerade as authorized users may gain inappropriate access. This risk may impact many types of systems and must be addressed through strong procedures, education, and awareness programs.

A user may be identified by something that they know, something that they have, or something that they are (e.g., biometric device such as a fingerprint). Single-factor authentication involves just one identification mechanism. This is usually something that they know such as a username and password. When a valid username and password are submitted to the operating system the user account is looked up in the security account manager (SAM) database. If the account exists, the submitted password is run through a one-way hash function. This one-way hash of the password is compared to the hash in the SAM database. If there is a match, a security token, that identifies the user and to what groups they belong, is built for the session. Changes to a user's rights require that they log out of the OS and re-logon for the new rights to take effect.

There are three locations from which users can authenticate themselves to Windows NT:

- From the console
- From inside network
- From outside the network

From the console, the basic user authentication in Windows NT is the username and password combination. This is done by first pressing control-alt-delete, the so-called secure attention sequence (SAS) that activates the Winlogon process, at the console keyboard.

This key combination is used because it is a set of keys that have not been used as a 'hotkey sequence' prior to this usage to avoid conflicts with existing applications. Another reason for this is that the sequence can be implemented at a very low level of the operating system, which helps to protect users from Trojan horse programs. Trojan Horse programs are always a potential problem in any operating system that uses a password-based authentication method. One form of a Trojan Horse attack substitutes the legitimate logon program for a Trojan program that steals the user’s password, can somehow record it, and relays it back to the creator.

From another location in the domain, the user can logon remotely. Historically, the remote logon process in many systems involves clear-text transmission of the user's identification and password. This transmission can be monitored and reused to access a user account. This has been a problem for many years with the TCP/IP-based network utilities, such as telnet, that send passwords over networks in clear text. Network administrators (and others) can use debugging and performance monitoring tools to capture the readable identifier and password. The Windows NT "netlogon" process uses encryption to protect the remote logon process. The entire logon process is described in the Logon Process section of the Security Architecture heading on page 16. For non-NT systems, there are other utilities to secure the logon process; for example, the Microsoft User Authentication Module for Macintosh uses the Microsoft Challenge Authentication Protocol (MS-CHAP) installed on the client to encrypt the logon session.

For access from outside the network, Windows NT provides the Remote Access Service, or RAS. RAS allows Windows workstations to access NT servers across standard phone lines (POTS, Frame Relay, or ATM) or other asynchronous connections, X.25 packet switched networks, or ISDN lines. RAS uses remote node systems to provide this capability. Remote node systems run the application on the remote user's computer and treat the connection line as an extension of the local area network, sending LAN-style traffic, such as requests for file and print services, over the line, which allows for greater flexibility and security. Because RAS treats the connection line as an extension of the LAN, it is designed to support Windows NT’s security model, complete with trust relationships and centralized domain administration.

RAS supports a number of authentication protocols for dial-in clients. They include:

- The password authentication protocol (PAP) that sends passwords in clear text
- SPAP, that uses two-way encryption for use with the Shiva LAN Rover product
- The US federal government's data encryption standard (DES)
- The challenge-handshake authentication protocol (CHAP)
- Microsoft's version of this protocol (MS-CHAP)

Windows NT also supports two-factor authentication. Users can optionally use token devices that generate one-time passwords. Windows NT will also support the use of SmartCards. These can take the form of PC cards (which plug into a PCMCIA device) or IC Chip cards. Through the use of device drivers and additional hardware (i.e., card readers), the authentication process can be further secured. In addition, SmartCards can store cryptographic key material that can provide digital signatures for authentication, integrity, and non-repudiation, and encryption that provides confidentiality to network activity. Microsoft is working with a number of hardware vendors to develop implementations based on ISO standards as part of the Personal Computer/SmartCard Workgroup. Applications can use the CryptoAPI (see the discussion on CryptoAPI on page 53) to integrate the benefits of SmartCard technology.

Windows NT Domains and Trust Relationships

A domain is a set of computers with a central security authority, the primary domain controller (PDC), that grants access to a domain. Usually a domain also contains one or more backup domain controllers (BDC) that provide distributed authentication services to provide continuing authentication services in the event of failure in the PDC, as well as load balancing for authentication services. As a rule many types of systems may join a domain, but the PDC and the BDC must be Windows NT systems, due to the compartmentalized security they can offer. A domain can be set up to ease viewing and access to resources, to share a common user account database and common security policy, and to allow administrators to enforce a common security stance across physical, divisional, or corporate boundaries. Once users are authenticated to the domain, using either the PDC or a BDC, they can gain access to the resources of the domain, such as printing, file sharing or access to applications, across all of the servers within the domain.

This concept of a domain-wide user account and password eliminates the need for every machine to provide its own authentication service. Instead, the authentication processes is passed through to the domain controllers for remote authentication against that user account database. This allows machines to be dedicated to servicing individual applications or programs without the overhead of authentication.

The primary function of the PDC is to maintain the security database. A read-only copy of this database is replicated to each BDC on a regular basis to maintain consistency in the environment. Because of the importance of maintaining the security database on the PDC and BDC, strict logical and physical access controls should be implemented.

Trusts are one way relationships that can be set up between domains to share resources and further ease administration. These relationships allow a user or groups to be created only once within a set of domains, yet access resources across multiple domains. There are a number of trust models used to configure domains.

The first is the single domain model with only one PDC and, by definition, no trust relationships.

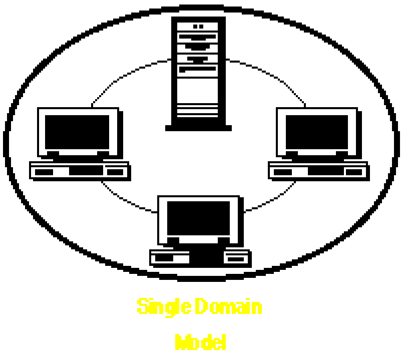

Figure 4: Single Domain Model

The next model is the master domain model for companies who desire centralized security administration. In this configuration, all domains, known as user or resource domains, trust the master domain. The master domain maintains security resources for all of the domains within this structure. This configuration can support up to 15,000 users. There is one trust relationship for every domain that trusts the master domain.

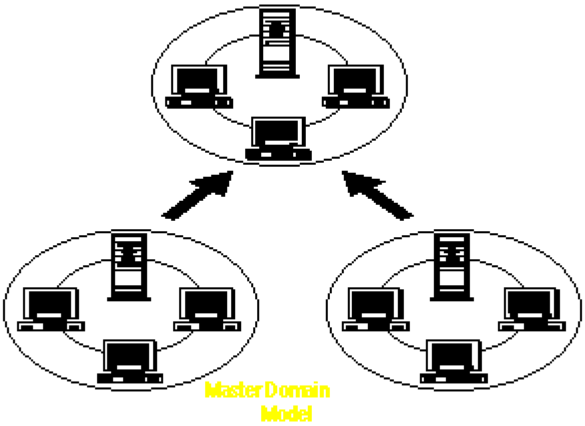

Figure 5: Master Domain Model

The multiple master domain model is designed for larger organizations that desire some centralized security administration. With more than one master domain, administration needs increase due to the need to create all network accounts on each master domain. The two master domains in this case trust each other, while the resource domains have one trust relationship with each of the master domains.

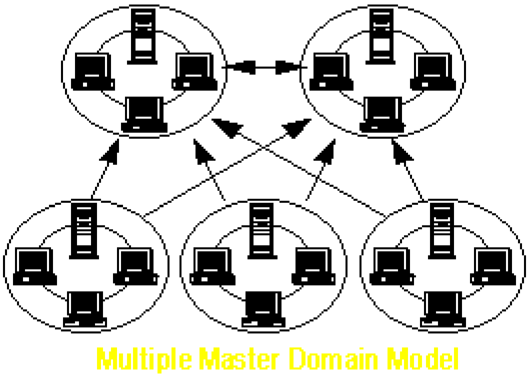

Figure 6: Multiple Master Domain Model

Finally, there is the complete trust model. This is designed for larger companies that desire totally decentralized security administration. This configuration presents considerable risk as all domains have two-way trust relationships with each other. This concept essentially provides peer-to-peer domains.

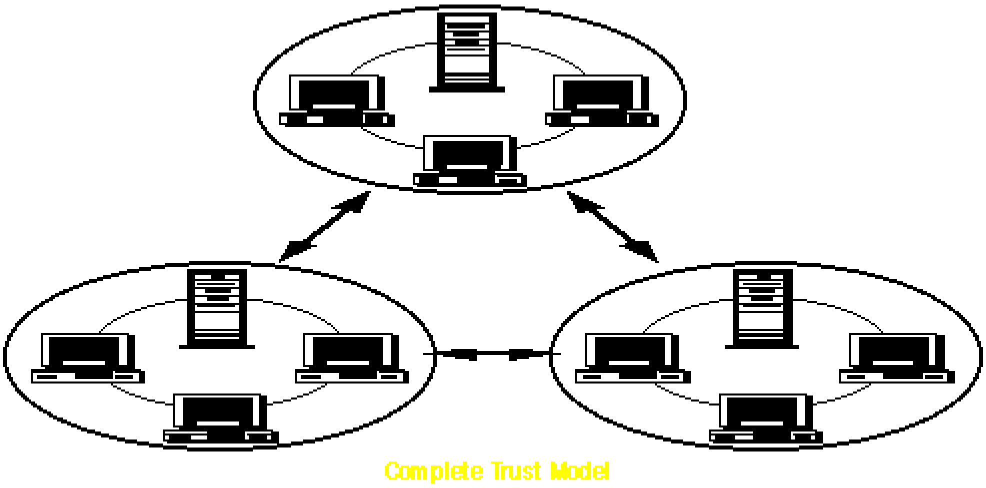

Figure 7: Complete Trust Model

Supported Network Transport Protocols

Windows NT works with both Microsoft's networking protocols and is compliant with other standard networking and communication protocols. One of the top considerations for configuring a Windows NT server is what protocols to install and use. Protocols supported include:

- TCP/IP
- NetBEUI
- NWLink (IPX/SPX)

A major challenge faced by operating system vendors is how to make a secure, standards-based product while possibly relying on old, insecure protocols. This has been an on-going issue for all operating system vendors.

Essentially, Windows NT does not attempt to fix weaknesses in any protocol. Compensating controls, such as the use of link- or application-level encryption, may be a necessary addition for security conscious organizations.

Security Certifications

The US Government wrote a series of manuals on computer security over the past few decades, each with a different color cover. This "Rainbow Series" of manuals includes how to design, build, choose, analyze, and operate a 'trusted system.' The Orange book (so called for the bright orange cover) was released in December 1985 and discussed what criteria to use to evaluate a trusted system. Additional manuals were subsequently produced that expanded the general terms used in the Orange book. They are the Red book, that interprets the Orange book with relation to networked systems, and the Blue book that interprets the Orange book with relation to subsystems.

The Orange book divides security into four sections, D through A. The D level is 'minimal protection', while class A is 'verified protection.' In the C class there is C1, 'discretionary security protection' and C2, 'controlled access protection.' Each level states the requirements for the following areas: Security Policy, Accountability, Assurance, and Documentation, and defines what a system must be able to do in each area to meet the requirements of that level.

When a system is evaluated against these criteria, a specific hardware and software configuration is created and used for the evaluation. Once evaluated, government organizations that require the appropriate level of security can purchase the evaluated systems. The D level has no criteria and is reserved for systems that were evaluated but did not meet the criteria for a higher evaluation class. The C2 level is the minimum acceptable level for certain government uses.

Due to required rating levels for government usage, the perception grew in the public that if it was good enough for Department of Defense use, it was good enough for commercial use. However, many people today speak of "C2 Security" without understanding the requirements or implications of the certifications. Some of the common misconceptions include:

- If the operating system is certified as C2, it will be C2 in any environment or configuration
- The C2 standards are appropriate and applicable for all commercial use
- The C2 standards include such areas as specific password controls and cryptography usage

The above are all false.

The entire section defining the C2 requirements is just three pages long. It states that the user is required to be individually accountable for their actions through logon procedures, the ability to audit security-related events, what the audit records will include, and the requirements of resource isolation.

ITSEC, is the Untied Kingdom’s equivalent of the US DOD National Computer Security Center. Conceptually their rating system is the same, except that they divide the ratings into both a functional class (F-C) with F-C2 being equivalent to C2, and evaluation level (E0 to E6) that defines the level of confidence that a product will meet the functional criteria in as many scenarios as possible. Under this rating scheme, Windows NT has received an FC2/E3 rating for both the client side and the server side. More detail on these rating levels are available at <www.itsec.gov.uk>.

Microsoft, with intentions of serving the government marketplace and with an understanding of the public's impression of the C2 level of security, designed the architecture of Windows NT to be in compliance with the criteria for Orange book C2 certification, including Red and Blue book compliance. Controls were incorporated that include: verification of user actions against the security database, the use of a session token, protection of that security database, the use of a username and password combination to access the system, the ability to audit events on a user-by-user basis for success and failure, access control lists to define access to objects, the NTFS file system to enforce access controls to objects in the system, use of the security reference monitor to control object reuse, memory space protection, and other integrated features. Note that physical control over access to the computer system plays a critical role in C2 compliance, and security in general, but is not a feature that can be built into the operating system.

C2 - FC2/E3

As of August 1995 Windows NT 3.5, Service Pack 3 (without networking installed) passed the certification requirements of the NCSC C2 Orange book level. Currently Windows NT 4.0 with Service Pack 3 is under evaluation. Windows NT 3.51 Workstation with Windows NT 3.51 Server were rated by ITSEC to meet their F-C2/E3 standard levels in October 1996. Windows NT 4.0 has been submitted for ITSEC review. One important point relating to C2 certification is that due to the rigorous level of testing the government does to determine compliance, the testing can take a long period of time. During this period, it is possible for patches, hot fixes, and service packs to be released. If the vendor would like these upgrades included in the evaluation, the process is significantly extended to allow for a review of the patch and the other code that the fix interacts with to make sure that the fix does not introduce a new security vulnerability while fixing a different problem. During an evaluation for either C2 or E3 certification, the source code of the system is available for review as well as the overall development process.

Some of the critical concepts to understand are:

- **Out of the box many operating systems (including Windows NT) are considered insecure.**
- **C2 compliance may or may not meet an organization's security need.**
- **A C2 level security configuration (this includes no floppy drive, and no network connectivity) may be impractical or inappropriate to use in many organizations.**
- **There are other controls such as physical and monitoring controls that must be addressed for compliance but are not operating system components.**
- **Availability, which is often critical in many corporate environments, is not one of the**

criteria for C2 certification.

- **An organization must assess the level of risk associated with the data they are attempting to protect, have a policy in place to define what security level is appropriate in their environment, and have monitoring controls in place to determine if the policy is being complied with.**
- **Using these criteria, a company can appropriately decide if the level of security they have implemented is too much, appropriate, or needs additional controls, such as link level cryptography between a client and a server. In this light, the question is not "is the product C2 certified" but "will this operating system, alone or with additional OEM or third party tools, meet the security needs of my organization?".**

Windows NT Server Attacks and Defenses

As its usage across business and industry increases, Windows NT server has come under closer scrutiny than ever regarding possible security flaws and holes. In the following table, we examine the various attacks on the Windows NT Server operating system and the defenses put in place in attempts to mitigate them.

Windows NT has been shown vulnerable to various Denial of Service (DOS) and other attacks that either attempt to retrieve sensitive information or attempt to gain access with permissions greater that the attackers own. To provide a secure environment, Microsoft provides fixes in the form of patches and service packs. After being notified of the exposure presented, Microsoft issues fixes. Listed below are some of the more wide-spread attacks that have been identified and the associated fix that has been released.

Attack / Method	**Defense**
Access Gaining and Information Gathering	
Anonymous User Connections (Red Button) is used to gain information regarding the administrative account and the network shares that are available.	Insert key into registry that prevents the anonymous user from making a network connection to the server: HKLM\System\CurrentControlSet\Control\LSA\RestrictAnonymous\* Type: REG_DWORD Value: 1
Remote Registry Access attempts to gain access to the registry, either to retrieve passwords or to change system settings.	Remote registry access is prevented in Windows NT Server version 4.0 by the addition of a registry key. This key is present by default in a new installation of Windows NT Server 4.0, but is not present by default in Windows NT Workstation 4.0. It may also not be present in a computer that has been upgraded from Windows NT Server 3.51. HKLM\System\CurrentControlSet\Control\SecurePipeServers\winreg
Password Theft and Cracking is an attempt to capture hashed passwords and crack them in order to gain further access to a system.	Increase password encryption in the SAM by applying the features of SP 3. Remove anonymous access to the system and tighten registry security.
Weak and Easily Guessed Passwords	Enforce a strong password policy from the domain controller using passfilt.dll. Passfilt.dll is available from Service Pack 2

Attack / Method	**Defense**
	onward. Details on how to implement passfilt.dll are given in the Password Filtering section on page 54.
Rollback -- Rollback.exe is included with Windows NT 4.0. It is a tool that forces the systems configuration back to installation settings.	Rollback may be used as a Trojan Horse, and it should be deleted from all systems.
GetAdmin -- The GetAdmin program was recently released from a Russian source. GetAdmin allows a regular user to get administrative rights on the local machine. A follow on to GetAdmin that may bypass the hotfix has just been released during this writing.	A security hotfix to patch both GetAdmin and the follow-on issue have been released by Microsoft.
Services running under System context could be used to gain access to the registry and other parts of the system as “SYSTEM”.	Run Services as accounts other than system wherever possible.
Unsecured Filesystem access using either a DOS or Linux-based tool gives access to the NTFS filesystem without any security controls.	Physically secure the server to prevent access to the diskette drive.
Server Message Block (SMB) NetBIOS access. These access ports that are required for file sharing may present an access path, especially when exposed to the Internet or when used in conjunction with a UNIX server running the Samba toolset.	Apply service pack 3 and disable TCP and UDP ports 137, 138, and 139 on any server connected to an outside network.
Denial of Service	
Telnet to unexpected ports can lead to locked systems or increased CPU usage. Telnet expects connections to be made to port 23 only. By default, Windows NT does not support a telnet daemon..	Apply Service Pack 2 or 3.
The Ping of Death (Large ping packet). An attack that has affected many major operating systems has also been found to affect	This problem was resolved in SP2.

Attack / Method	Defense
Windows NT. The Ping of Death is caused by issuing ping packets larger than normal size. If someone was to issue the ping command, specifying a large packet size (>64 bytes), the TCP/IP stack will cease to function correctly. This effectively takes the system off-line until rebooted. Most implementations of ping will not allow a packet size greater than the 64 byte default, however Windows '95 and NT do allow this exception and can therefore cause or be vulnerable to such a system denial. A recent version of this problem has affected Windows NT Server version 4.0 SP3 systems that run IIS and are exposed to the Internet. This was due to a fragmented and improperly formed ICMP packet.	A new hot fix has been released, post SP3, called the icmp-fix.
'SYN' Flood Attack -- A flood of TCP connection requests (SYN) can be sent to an IIS server that contain “spoofed” source IP addresses. Upon receiving the connection request, the IIS server allocates resources to handle and track the new connections. A response is sent to the "spoofed" non-existent IP address. Using default values, the server will continue to retransmit and eventually deallocate the resources that were set aside earlier for the connection 189 seconds later. This effectively ties up the server and multiple requests can cause the IIS server to respond with a reset to all further connection requests.	Service Pack 2 provides a fix to this vulnerability.
Out of Band Attacks - Out of Band (OOB) attacks, where data is sent outside the normal expected scope have been shown to affect Windows NT. The first OOB attack was identified after Service Pack 2 (SP2) and a patch was released that was also included in SP3. This attack caused unpredictable results and sometimes caused Windows NT to have trouble handling any network	Apply service pack 3 and the subsequent OOB-fix.

Attack / Method	Defense
operations after one of these attacks. Since the release of SP3, another problem has been identified in the TCPIP.SYS network driver that caused Microsoft networking clients to remain vulnerable to variations of the OOB attack, coming from the Apple Macintosh environment. The OOB attack crashes the TCP/IP protocol stack, forcing a reboot of Windows NT. A subsequent hotfix was released to counter this attack.	

Table 4: Windows NT Attacks and Defenses

Services That Enhance or Impact Security

Impact of the Internet on Security

The Internet evolved from the Defense Department's Arpanet, which was first created in the late 1960s. In 1991, commercial traffic was allowed on it for the first time. With commercial use and the subsequent development of the hypertext transport protocol and the World Wide Web that uses it, companies began to connect their corporate WANs to the Internet. The very visible connectivity and accessibility to corporate networks by large numbers of people has created a number of changes in corporate views of data security. The primary impact was one of awareness. In a very short time, non-technical people started talking about technology. They also stated asking about the security of their connections. The hype and misinformation surrounding the Internet's features and risks have created the need for technology solutions and education about technology and security. Anyone can become a content publisher almost overnight. Sharing data with employees, strategic partners, customers, and even competitors, has become very easy to do. Naturally, this introduces or enhances the risks to an organization’s data.

Internet Information Server

The addition of Internet Information Server (IIS) to the base Windows NT operating system has provided Windows NT Server with new functionality as well as exposing Windows NT to the security risks of the Internet. IIS is integrated with the Windows NT operating system making it an alternative to expand NT Servers to Web servers for intranet and the Internet. IIS also includes standard TCP/IP servers for FTP and Gopher. This web client-server model provides a method to utilize Windows NT to provide information to people on the internal network as well as on the Internet.

There are many well known security risks associated with the Internet and IIS allowed Windows NT to be exposed to them. However, because IIS is coupled with Windows NT Server, it allows for the use of the security features found in the operating system.

In addition, other applications and protocols have been developed in an attempt to limit these security exposures. A few of these applications and protocols have been explored below as an example of Microsoft's role in Internet technologies. As always, any system exposed to the Internet should be protected using multiple layers of security.

Proxy Server

The Microsoft Proxy Server offers features such as site filtering, access control, request logging, multiple Internet protocol support, caching, and remote administration. This application also integrates with IIS and the Windows NT operating system. The Proxy Server is an optional product, not included with the base operating system.

The proxy server assists in preventing network penetration by masking the internal network from other external networks. Client requests can be verified to be sure that they are coming from the internal network. IP packets with destination addresses not defined are prevented from accessing computers on the internal network. This helps to prevent spoofing attacks. Filtering can limit access to specified network addresses, address ranges, subnet masks, or Internet domains. The proxy server provides two levels of activity or security logging. User-level authentication is provided between the client and proxy server. Specific protocols can be secured at an individual or group level, or the option to entirely disable access to protocols exists.

Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL) is supported by the Microsoft Proxy Server. This allows a secure session between the server and a client computer. SSL 3.0 is a protocol that provides for mutual authentication and confidentiality between Web browsers and Web Servers. SSL provides a security "handshake" that is used to initiate the TCP/IP network connection. This handshake results in the client and server agreeing on the level of security (i.e. algorithm and key length selection) that they will use and identifies both parties. SSL requires the use of digital certificates and provides both server-side and client-side certificates for the connection. SSL encrypts and decrypts the byte stream of the application protocol being used (for example: HTTP). This means that all the information in both the HTTP request and the HTTP response are fully encrypted, including the Universal Resource Locator (URL) that the client is requesting, any submitted form contents (such as credit card numbers), any HTTP access authorization information (user names and passwords), and all the data returned from the server to the client.

Server-Based Routing

Microsoft has introduced the Routing and Remote Access Service. The new routing features integrate with the Microsoft Proxy Server and provide an added layer of security. Windows NT's routing features support for RIP, OSPF, and DHCP Relay protocols on IP networks and RIP and SAP protocols on IPX networks.

The new service provides the rough equivalent of packet filtering security that can be found on many hardware-based routers. The filtering can be used for packet layer network security, and, when used with Microsoft Proxy Server, complements the application layer security. Filters are configured on an exception basis. Users can configure the filter to pass only the packets from the routes listed, or pass everything except the packets for the routes specified.
.
Another security feature provided is Remote Authentication Dial-In User Service (RADIUS). This provides another security and accounting option that can be used with this service. With RADIUS client support, an administrator can elect to use Windows NT Server domain-based database for user authentication or, can instead elect to use some other RADIUS server

database to perform the authentication.

Point-to-Point Tunneling Protocol (PPTP)

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that facilitates the secure transfer of data from a remote client to a private enterprise server by creating a virtual private network (VPN) across TCP/IP-based data networks. The PPTP protocol encapsulates data for transmission over TCP/IP-based networks.

PPTP provides a form of secure and encrypted communications over public telephone lines and the Internet. PPTP eliminates the need for expensive, leased-line or private enterprise-dedicated communication servers because PPTP can be used over standard telephone lines.

Authentication of remote PPTP clients are done by using the same authentication methods used for any RAS client dialing directly to a RAS server. Microsoft's implementation of RAS supports the Challenge Handshake Authentication Protocol (CHAP), the Microsoft Challenge Handshake Authentication Protocol (MS-CHAP), and the Password Authentication Protocol (PAP) authentication schemes. After authentication, all access to a private LAN continues to use the Windows NT-based security model. These methods of user authentication are discussed in the section User Authentication on page 22.

For data encryption, PPTP uses the Remote Access Server (RAS) "shared-secret" encryption process and requires the use of the MS-CHAP authentication process. The data packets are encrypted and then encapsulated into a larger packet for routing over the Internet to the PPTP server.

Network security can also be increased by enabling PPTP filtering on the PPTP server. When PPTP filtering is enabled, the PPTP server on the private network accepts and routes only PPTP packets from authenticated users. This prevents all other packets from entering the PPTP server and private network.

Windows NT Server Security Features

Windows NT is designed to provide an operating system that could be used in many types of implementations, from local application servers and LAN file servers, to remote access servers and Internet/Intranet web servers. Windows NT has features for security designed to provide the user with choices of a limited or extensive control implementation, depending on the business needs. The following table, Table 5, lists both the features that either control or implement security and describes those features.

Feature	Description
Local Security Authority (LSA)	The LSA is also referred to as the security subsystem and is the heart of the Windows NT Server subsystem. The LSA provides the following services: • Creates access tokens during the logon process • Enables Windows NT Server to connect with third party validation packages. • Manages the security policy • Controls the audit policy • Logs audit messages to the event log
Security Account Manager (SAM)	The SAM maintains the security account database. SAM provides user validation services which are used by the LSA. SAM provides a security identifier for the user and the security identifier of any groups which the user is a member. SAM operates as part of the Kernel.
Security Account Database (SAD)	The SAD contains information for all user and group accounts in a central location. It is used by the SAM to validate users. Duplicate copies of the SAD can reside on multiple servers depending on whether a workgroup or domain model is implemented and the type of domain model implemented. Passwords stored in the SAD are stored using a 128-bit cryptographically strong system key.
Security Identifiers (SID)	SIDs are created by the security account manager during the logon process. They are retired when an account is deleted. If an account name was created with the same name as an account that was previously deleted, the SID created will be different from the SID associated with the deleted account.
Security Reference Monitor (SRM)	The SRM is the Windows NT Server component responsible for enforcing the access validation and audit generation policy held by the LSA. It protects resources or objects from unauthorized access or modification. Windows NT Server does not allow direct access to objects. The SRM

Feature	Description
	provides services for validating access to objects (files, directories, etc.), testing subjects (user accounts) for privileges, and generating the necessary audit message. The SRM contains the only copy of the access validation code in the system. This ensures that object protection is provided uniformly throughout Windows NT, regardless of the type of object accessed.
Discretionary Access Controls	Discretionary access controls provide resource owners the ability to specify who can access their resources and to what extent they can be accessed.
Access Tokens	Access tokens are objects that contain information about a particular user. When the user initiates a process, a copy of the access token is permanently attached to the process.
Access Control Lists (ACLs)	ACLs allow flexibility in controlling access to objects and are a form of discretionary access control. They allow users to specify and control the sharing of objects or the denial of access to objects. Each object's ACL contains access control entries that define access permissions to the object.
Logon Process	The interactive logon process is Windows NT Server's first line of defense against unauthorized access. In a successful logon, the process flows from the client system to the server system without exposing the user's password in clear text over the network. The entire logon process is described in the section entitled Logon Process on page 16.
The Registry	The Windows NT Server Registry is an access controlled database containing configuration data for security, applications, hardware, and device drivers. The registry is the central point for storing these data. The registry contains all user profile information as well as the hashed user password.
Event Logging (Auditing)	Windows NT Server auditing features record events to show which users access which objects, the type of access attempted, and whether or not the attempt was successful. Auditing can be applied to: • System events such as logon and logoff, file and object access, use of user rights, user and group management, security policy changes, restarting and shutting down the system, and process tracking • File and directory events such as read, write, execute, delete, changing permissions and taking ownership • Registry key access to subkeys • Printer access events such as printing, taking full control, deleting, changing permissions, and taking ownership

Feature	Description
	• Remote Access Service events such as authentication, disconnection, disconnection due to inactivity, connection but failure to authenticate, connection but authentication time-out, disconnection due to transport-level errors during the authentication conversation, and disconnection due to inability to project onto the network • Clipbook page events such as reading the page, deleting the contents of the page, changing permissions, and changing the audit types. • Events of significance can be sent to a pager interface to notify security and systems staff
Event Logs	Three logs record system, security, and application related events: 1. The system log records errors, warnings, or information generated by the Windows NT Server system. 2. The security log records valid and invalid logon attempts and events related to the use of resources such as creating, opening, or deleting files or other objects. 3. The application log records, errors, warnings, and information generated by application software, such as an electronic mail or database application. The size and replacement strategy can be modified for each of the logs. Each logged event's details can be displayed.
Process Isolation	Windows NT was designed to provide process isolation in order to prevent individual processes from interfering with each other. This is accomplished by providing each process its own memory space with no access to any other processes' memory. This segregation of memory is also designed to prevent data from being captured from the memory space. There is an option to overwrite an individual user's swap or temporary disk space after logout to prevent anyone from reading that user's temporary files and data.
User Account Security	User account security policies are managed through the user manager, and consist of account policies and user rights policies. • Account policy controls the way passwords must be used by all user accounts. The major account policy controls include minimum and maximum password age, minimum password length, password uniqueness, forcible disconnection beyond logon hours, and account lockout. • User rights policy allows the granted user to affect resources for the entire system. The basic rights offered by Windows NT Server include access from a network, backing up, changing the system time, remote forcible shutdown, local log on, managing the audit and security log, restoring files, shutting down the system, taking ownership of objects.

Feature	Description
	Windows NT Server also contains many advanced rights. In total, there are twenty-seven rights that may be assigned to users.
Built-in Accounts	Windows NT Server offers two built-in accounts: the guest account and the administrator account. These accounts were created for specific uses and are by default members in a number of default groups. The guest account is disabled by default.
User Account Properties	The user properties feature allow the administration of user accounts, passwords, password policies, group membership, user profiles, hours of logon, the workstations from which the user can log on, and the account expiration date. In addition, password filtering can be implemented to increase the strength of password security policy.
User Profiles	User profiles enable the Windows NT Server to structure and manage the user's desktop operating environment, and present the identical environment without regard to the workstation. This file is loaded upon logon. The user profile editor allows disabling Run in the file menu, disabling the Save Settings Menu item, show common groups, change the startup group, lock program groups, restrict access to unlocked program groups, and disable connecting and removing connections in the print manager.
Home Directories	Home directories can be assigned to each user for storage of private files.
Logon Scripts	Logon scripts are executed upon logon by a user. They provide the network administrator with a utility for creating standard logon procedures.
Groups	Groups allow an administrator to treat large numbers of users as one account. Windows NT Server utilizes two types of groups in its tiered administration model: • Local groups are defined on each machine and can contain both user accounts and global groups. Windows NT supplies a number of built-in local group accounts. • Global groups are defined at the domain level and can contain only user accounts from the local domain, but not from trusted domains. Windows NT supplies several built-in, global group accounts.
Network Models	In a Windows NT network environment it is possible to implement two different network models: the workgroup model or the domain model. • The workgroup model allows peer to peer networking for machines that do not participate in a domain. Each Windows NT machine that participates in a workgroup maintains its own security policy and SAD.

Feature	Description
	• The domain model is an effective way to implement security and simplify administration in a network environment. The domain allows the sharing of a common security policy and SAD.
Trust Relationships	The domain model establishes security between multiple domains through trust relationships. A trust relationship is a link between two domains causing one domain to honor the authentication of users from another domain. A trust relationship between two domains enables user accounts and global groups to be used in a domain other than the domain where these accounts are located. Trusts can be uni- or bi-directional and require the participation of an administrator in both domains to establish each directional trust relationship.
Primary and Backup Domain Controllers	Windows NT Server provides domain authentication service through the use of primary and backup domain controllers. If communications to the primary domain controller break, the backup domain controllers will handle all authentication. A backup domain controller may be promoted to a primary domain controller if necessary.
Replication	Windows NT Server uses replication to synchronize the SADs on various servers. This process is automatic. Replication is not restricted to the SAD, but can be used to create and maintain identical directory trees and files on multiple servers and workstations. The replication feature contains a security tool to control the import and export of files and directories.
Server Administration	The server manager tool enables the following types of administrative activities: • Display the member computers of a domain • Select a specific computer for administration • Manage server properties and services, including start and stop services and generate alerts • Share directories • Send messages to systems These administrative functions require administrative access.
NTFS	NTFS is the more secure of the two writable file systems supported by Windows NT Server. NTFS is the only file system to utilize the Windows NT file and directory security features. NTFS is a log-based file system that offers recoverability in the event of a disk fault or system failure. The next major release of the operating system will provide an option for file-level encryption.

Feature	Description
Legal Notice	The legal notice feature is provided to strengthen the legal liability of individuals who may attempt to access a system without authorization. The feature displays a message to the user after the CTRL+ALT+DEL keystroke combination during the logon process. When the legal notice appears, the user must acknowledge the notice by selecting the OK button in the message box presented.
Fault Tolerance	Windows NT Server has fault tolerance features that can be used alone or in combination to protect data from potential media faults. These features are disk mirroring, disk duplexing, disk striping with parity, and sector hot-sparing.
Tape Backup	The Tape Backup enables backing up and restoration of files and directories. Backups can be full, incremental, differential, custom, or on a daily basis for those files changed on the day of the backup.
Last Known Good Configuration	The last known good configuration feature allows the restoration of the system to the last working system configuration. When used, it discards any changes to the configuration since the last working system configuration. This feature is automatically updated after any system boot.
Emergency Repair Disk	The emergency repair disk allows the restoration of the system to its initial setup state. The emergency repair disk can be used if system files are corrupt and the user is unable to recover the previous startup configuration. Securing the emergency repair disk is of utmost importance as it contains a copy of key pieces of the security accounts database.
Uninterruptible Power Supply Service (UPS)	The UPS feature allows for the connection of a battery operated power supply to a computer to keep the system running during a power failure. The UPS service for Windows NT Server detects and warns users of power failures and manages a safe system shutdown when the backup power supply is about to fail.
Network Monitor	The Network Monitor allows examination of network traffic to and from a server at the packet level. This traffic can be captured for later analysis, making it easier to troubleshoot network problems.
Task Manager	The Task manager is tool for monitoring application tasks, key performance measurements of a Windows NT Server-based system. Task manager gives detailed information on each application and process running on the workstation, as well as memory and CPU user. It allows for the termination of applications and processes.
Performance	The performance monitor tool enables the monitoring of system capacity

Feature	Description
Monitor	and prediction of potential bottlenecks.
Network Alerts	Alert messages can be sent to designated individuals. These messages can report on security related events, such as too many logon violations or performance issues.
CryptoAPI	This set of encryption APIs allows developers to develop applications that will work securely over non-secure networks, such as the Internet.
Point-to-Point Tunneling Protocol (PPTP)	PPTP provides a way to use public data networks, such as the Internet, to create virtual private network connecting client PCs with servers. PPTP provides protocol encapsulation and encryption for data privacy.
Distributed Component Object Model (DCOM)	Windows NT 4.0 includes DCOM, formerly known as Network OLE, that allows developers and solution providers use off-the shelf and custom-created OLE components to build robust distributed applications. Most importantly, it utilizes Windows NT Server's built-in security. It addresses a problem that was frequently associated with OLE applications trying to run as services under Windows NT: Windows NT Server's built-in security did not let OLE services communicate between applications because most applications are launched from a desktop running a different security context from the services. Using DCOM, Windows NT 4.0 now allows communication between different security contexts.
Windows NT Diagnostic Tool	The Windows NT diagnostic tool is used to examinethe system, including information on device drivers, network user, system resources.
Services Administration	The Service Manager enables the access and administration of network and operating system services.
Remote Access Services (RAS) Administration Tools	The RAS administration tools control the remote connection environment. The following tools are used in the RAS configuration and administration process: • Network Settings enables the installation and configuration of network software and adapter cards and the ports in which they reside. • Network Configuration controls the RAS inbound and outbound protocols as well as encryption requirements. Each protocol has subsequent dialog boxes with configuration and control features. • The Remote Access administration tool enables monitoring of specific ports, administration of remote access permissions, and configuration of any call back requirements.

Feature	Description
Internet Information Server (IIS)	IIS is an add-on to Windows NT 4.0. Integration of IIS with NT 4.0 allows IIS to have full use of NT 4.0 server security and directory services. The integration supports logging server traffic to NCSA Common Log File Format, as well as any ODBC database. IIS provides Web, FTP and Gopher services to the Windows NT system.
TCP/IP Support	Windows NT Server supports the TCP/IP protocol and IP address format. The TCP/IP Configuration tool administers TCP/IP as well as SNMP, DHCP, and WINS. The Configuration tool also controls IP routing. Traditional TCP/IP commands such as ARP, NBTSTAT, NETSTAT, PING, TRACERT and the UNIX 'R' commands are supported.
C2 Tool	The C2 tool provides guidance for securing the Windows NT Server to the C2 security standard.

Table 5: Windows NT Security Features

Defining Security Settings

Windows NT allows modifcation of the default security settings . The following summarizes a few of the options available and possible alternatives to increasing network security:

Account Policies

The user account policy controls the password characteristics for all user accounts across the domain. The table below, Table 6, details Windows NT Account Policy options and recommendations:

NT Policy Feature	Policy Option	Recommendation
Maximum Password Age	Password never expires Expires in *x* days	Password expires in 30 - 60 days.***
Minimum Password Age	Allow changes immediately Allow Changes in *x* days	Allow changes in 7 days.
Minimum Password Length	Permit blank password At least *x* characters	Password at least 6 characters.
Password Uniqueness	Do not keep password history Remember *x* passwords	Remember 10 passwords.

NT Policy Feature	Policy Option	Recommendation
Account Lockout	No account lockout Account lockout	Account lockout selected.
Account Lockout	Lockout after *x* bad logon attempts	Lockout after 3 bad logon attempts.
Account Lockout	Reset count after *x* minutes	Reset count after 1440 minutes (24 hours)
Lockout Duration	Forever (until admin. unlocks) Duration *x* minutes	Select forever.
Forcibly disconnect remote users from server when logon hours expire	Selected Not selected	Tied to logon hours specified when user account was created.
Users must log on in order to change password	Selected Not selected	Select

Table 6: Account Policy

***60 days would be a permissible password change rate only if strong passwords are implemented. Strong passwords may only be implemented under Windows NT 4.0 at the domain controller. Strong passwords may implemented using the **passfilt.dll** program available under service pack 2 of Windows NT 4.0. The strong passwords provided by passfilt.dll are further described in the Password Filtering section on page 54.

User Accounts

When first installed, Windows NT server creates two default accounts:

Administrator Account The local administrator account is established during the installation of any version of Windows NT. This account is powerful and allows full access to the system. When an administrator account on a PDC is added to the Domain Admins group and the Domain Admins group is then added to the local Administrators group on a workstation, that account can then administer that particular workstation.

This administrator account cannot be deleted. It cannot be disabled from console login. It can, however, be disabled from network login. In the Windows NT version 4.0 resource kit, a utility program called passprop.exe exists. When utilized on a Windows NT system, this program allows the Administrator account to be locked from the network, just as any other regular user account.

In order to secure this account, it must be renamed an obscure value and only be used when necessary. It should be noted that renaming of the Administrator account does not completely obscure it from view. The Administrator account on every Windows NT system has the same SID, therefore making it possible to discover the identity a renamed administrator account. If it is necessary to use this account, it should be logged off immediately upon completion of that use. Administrators of Windows NT systems should be assigned their own account that is a member of the appropriate administrative group.

Security of the administrator account may be facilitated by creating an account called Administrator and granting it limited rights and forcing it to be locked out after several invalid access attempts.

Guest Account The guest account allows an anonymous logon to the domain. As the account is a member of the Everyone group, the account has the same access as the Everyone group. By default, the account is disabled and should remain disabled. For additional protection, a strong password should be assigned to the Guest account in case it is accidentally re-enabled. The Guest account will only function for anonymous access if it is enabled and has no password.

User Rights

Access to network resources are defined either by assigning rights to a user to perform specific tasks or by setting permissions directly to objects (files, directories, devices). As a rule, rights assigned to users override object permissions. The following details basic rights available on the system whose default groups should be carefully evaluated:

- *Access this computer from the network*. By default, this right is granted to the Administrators and Everyone group. Granting this right to the Everyone group allows all users to access the server from the network. As such, the Everyone group should not be assigned this right. A new group should replace the Everyone group in this instance and should include users or groups who should have network access.
- *Backup files and directories*. By default, this right is granted to the Administrators, Backup Operators, and Server Operators. Since this right overrides specific permissions placed on objects, users with this right have the ability to copy all files regardless of permissions. As such, carefully scrutinize the users and groups granted this right.
- *Force shutdown from a remote system*. By default, this right is granted to the Administrators, Server Operators, and Power Users in Windows NT Workstation group. This right allows the specified users or group members to send a the Windows NT system a shutdown command from any workstation or server on the network. As a recommendation, no group should ever be granted this right.
- *Log on locally*. By default, this right is granted to the Administrators, Backup Operators, Server Operators, Account Operators, Print Operators, and Internet Guest Account groups.

As this right allows the user to logon directly to the console of the server, only the Administrators group should be granted this right.

- *Shut down the system*. This right indicates that the specified users or group members can issue a shutdown command from the system's local console if they are logged on interactively to the console. By default, this right is granted to the Administrators, Backup Operators, Server Operators, Account Operators, and Print Operators. Only members of the Administrators and Server Operators should ever have a need for this right.

In addition to the basic user rights, Windows NT Server offers several Advanced User Rights. Administration of these rights should be carefully reviewed.

Registry Permissions

The registry stores configuration information for hardware, networking, device drivers, and software.

The registry should not be tampered with. There are no cautionary messages or validation of changes made to the registry. Any changes should only be made with extreme caution by an administrator, and be well documented.

The registry consists of five main sections called trees:

• HKEY_LOCAL_MACHINE	- hardware and software configuration
• HKEY_CLASSES_ROOT	- file associations
• HKEY_USERS	- default user profiles
• HKEY_CURRENT_USER	- current logged on user information
• HKEY_CURRENT_CONFIG	- current hardware configuration

Securing the Registry

Securing the registry will help prevent users and others from causing problems for Windows NT by changing registry values, inadvertently or otherwise. All users must have read access to certain portions of the registry in order to function in the Windows NT environment, but should not be able to change all registry values or make new registry entries.

There are some differences in the permission levels within the registry as compared to standard NTFS file and directory permissions. The registry supports three types of access permissions:

• Full Control	- users can edit, create, delete or take ownership of keys.
• Read	- users can read any key value but make no changes.
• Special Access	- users can be granted one or more of 10 specific rights to a specific key as described in the following table, Table 7:

Permission Level	**Description**
Query Value	Read the settings of a value entry in a subkey
Set Value	Set the value in a subkey
Create Subkey	Create a new key or subkey within a selected key or subkey
Enumerate Subkeys	Identify all subkeys within a key or subkey
Notify	Receive audit notifications generated by the subkey
Create Link	Create symbolic links to the subkey(s)
Delete	Delete selected keys or subkeys
Write DAC	Modify the discretionary access control list (DAC) for the key
Write Owner	Take ownership of the selected key or subkey
Read Control	Read security information within selected subkey

Table 7: Registry Subkey Permissions

- Disable remote registry editing by verifying existence or creating:
  HKLM\System\CurrentControlSet\Control\SecurePipeServers\winreg
- Disable anonymous access by creating:
  HKLM\System\CurrentControlSet\Control\LSA\RestrictAnonymous
  Type: REG_DWORD
  Value: 1
- Secure the root keys as shown in the following table:

Registry Key	Default Setting	Recommended Setting
HKEY_LOCAL_MACHINE	Administrators: Full Control System: Full Control Everyone: Read	Administrators: Full Control System: Full Control Everyone: Read
HKEY_CLASSES_ROOT	Administrators: Full Control Creator/Owner: Full Control System: Full Control Everyone:Read	Administrators: Full Control Creator/Owner: Full Control System: Full Control Everyone: Special Access as defined below
HKEY_USERS	Administrators: Full Control	No Change

Registry Key	Default Setting	Recommended Setting
	System: Full Control Everyone: Read	
HKEY_CURRENT_USER	Administrators: Full Control System: Full Control User: Full Control	No Change
HKEY_CURRENT_CONFIG (Windows NT 4.0 only)	Administrators: Full Control System: Full Control User: Full Control	No Change

Table 8: Registry Root Key Permissions

- Secure registry subkeys to limit the access of the Everyone group
    - Allow special access only to the Everyone group with only four (4) of the 10 permissions: Query Value, Enumerate Subkeys, Notify, and Read Control, using the following keys and subkeys:
        - HKEY_LOCAL_MACHINE\Software\Microsoft\RPC (and all subkeys)
        - HKEY_LOCAL_MACHINE \Software\Microsoft\WindowsNT\CurrentVersion

WARNING: Using the registry editor incorrectly can cause serious, system-wide problems that may require you to reinstall Windows NT. Microsoft cannot guarantee that any problems resulting from the use of the registry editor can be solved. Use this tool at your own risk.

System Enhancements that Affect Security

Security Features Added since version 3.51

The upgrade to Windows NT 4.0 brought about new changes, enhancements and additions. Many of these improvements directly affect the security of Windows NT 4.0. The following features were not included in Windows NT Server 3.51 and can now be found in Windows NT Server 4.0:

CryptoAPI (CAPI)

This set of cryptography APIs is designed to allow developers to create applications for secure communications over non-secure networks, such as the Internet. The CryptoAPI consists of modules called cryptographic services providers (CSPs). Each module performs some cryptographic services that developers can tap into. CryptoAPIs make it easier to implement security features in tasks and applications, such as creating applications that encrypt and decrypt files and creating applications that encrypt sign and verify messages.

Network Monitor

This network diagnostic tool allows you to examine network traffic to and from the server at the packet level. Users can capture network traffic for later analysis, making it easier to troubleshoot network problems. Network Monitor can also monitor unauthorized intruders by capturing and filtering network information. This includes allowing the view of frames related to a particular command that a hacker may be using, or by setting triggers to capture a code or sequence that a hacker might use.

System Policy and User Profiles

The system policy editor was added to Windows NT Server version 4.0. The policy editor allows the administrator to define system policies that affect individual or groups of users and machines. The policy editor can be used to set levels of access and control for user’s desktops, filesystems, and remote access. Policies are available during the logon process. Policies may be stored on the domain controllers or replicated to individual machines. Policies may be implemented on Windows NT Servers, Windows NT Workstations and Windows 95 systems.

Task Manager

The Task Manager is tool for monitoring application tasks and key performance measurements of a Windows NT Server-based system. Task Manager gives detailed information on each application and process running on the workstation. It also allows for the termination of applications and processes.

Improved Windows NT Diagnostic Tool

This diagnostic tool allows for examination of the system including information on device drivers, network use, system resources. It also provides certain statistics that are useful for security monitoring, such as: Server Password Errors, which track the number of failed logons attempted to a server, and Server Permission Errors, which is the number of times the clients have been denied access to files they were trying to open.

Communications Features

Point-to-Point Tunneling Protocol PPTP

This feature provides a way to use public data networks, such as the Internet, to create virtual private network connecting client PCs with servers. PPTP provides protocol encapsulation to support multiple protocols through TCP/IP connections and encryption for data privacy, making it safer to send information over non-secured networks. This technology extends the capacity of RAS to allow remote access and extend private networks across the Internet without the need to change client software.

Idle RAS Disconnect

This automatically terminates RAS connections after a certain period of time if no activity has occurred over the remote dial up communication link.

Updated Novell NetWare interoperability

Client and gateway services for NetWare are extended to support NDS, NetWare Directory Services. Added functionality includes browsing NDS resources, NDS authentication, and NDS printing. These services provide support for authentication to multiple NDS trees and processing logon scripts.

Internet

This addition of Microsoft Internet Information Server is an add-on to Windows NT 4.0. This allows IIS to have full use of Windows NT Server’s security model. In addition, the IIS server with Windows NT 4.0 eliminates the security problem that allowed anyone who had remote access to an IIS Web server to delete files for which the server had delete permission.

Windows NT 4.0 supports logging server traffic to detailed log files, as well as any ODBC-compliant database.

Windows NT 4.0 makes it easier to set up Secure Socket Layer (SSL) security by using the Key Manager tool.

The following enhancements corrected some of the potential security vulnerabilities found in Windows NT 3.51:

Remote Registry Access

Windows NT 3.51 allowed access to a system's registry from another machine on the network. Since Windows NT installed by default with the Everyone group given write access to much of the registry, any user who has an account anywhere in the domain could then manipulate the registry. Windows NT Server 4.0 comes with a key in its registry that disables remote registry access, other than to administrators. This key can also be added to Windows NT Workstation 4.0.

Default Settings

Default installation in Windows NT 3.51 left the Guest account enabled. In Windows NT 4.0 the Guest account is disabled on both workstations and servers.

FTP Service Directory

The FTP server supplied with Windows NT 3.51 allowed FTP users to change out of the current FTP directory, thereby possibly being able to access other directories that were properly secured with NTFS ACLs. The IIS FTP server in Windows NT 4.0 does not allow this.

Windows NT 4.0 Service Pack 3

Windows NT Server 4.0 Service Pack 3 (SP3) addresses a number of areas of the operating system, including many security items. The service pack contains such security enhancements as:

- Server Message Block (SMB) Signing
- System Key Encryption of Password Information (Stronger Encryption of the SAM)
- Password Filtering
- Restricting Unauthorized User Access
- Crypto API 2.0
- TCP/IP improvements to resist OOB Denial of Service Attacks

SMB Signing

The Server Message Block (SMB) authentication protocol is the file and printer sharing system in the NT environment. Service Pack 3 includes an updated version of the SMB protocol, which is used as the major component in the Common Internet File System (CIFS) protocol. CIFS complements services such as HTTP by providing a more sophisticated file sharing protocol. CIFS includes support for both anonymous transfers and for secure authenticated access to files and folders. The updated SMB Signing protocol has two main improvements that support mutual authentication between client and server, which closes the "man-in-the-middle" attack. It also supports message authentication, which prevents active message attacks.

A digital security signature is implemented into each SMB, which is then verified by both user parties to provide the authentication. If SMB file sharing is in use, it is a recommended practice to disable the guest account, requiring logging on with strong passwords and to check the permissions for folders (especially by the Everyone group).

There is an optional ability to support older versions of SMB. However, in order to use SMB signing, it must be enabled on both the client and the server. If SMB signing is enabled on a server, then clients that are also enabled for SMB signing will use the new protocol during all subsequent sessions. Clients who are not enabled for SMB signing will use the older SMB protocol. If SMB signing is required on a server, then a client will not be able to establish a session unless it is enabled for SMB signing.

Using a System Key to Strongly Encrypt Password Information

Service Pack 3 provides an enhancement to use encryption techniques to increase protection of account password information stored in the registry by the Security Account Manager (SAM). Windows NT stores user account information, including a cryptographic hash of the user account password, in the registry protected by access controls and a second layer of encryption.

Windows NT allows privileged users, who are administrators, access to all resources in the system. For general users who require enhanced security, strong encryption of account password information provides an additional level of security to prevent administrators from intentionally, or unintentionally, accessing password derivatives using registry programming interfaces.

Password Filtering

Service Packs 2 and 3 include a password filter (Passfilt.dll) that allows system administrators to increase password strength (which works well with improved SMB authentication). This dynamic link library filter is copied to %systemroot%\SYSTEM32 when SP3 is installed on the system.   This feature complements the built-in password policy.

The passfilt.dll requires passwords to be at least six characters long: they may not contain the user name or any part of the full name, and they must contain characters from at least 3 of the following 4 classes:

Class	Examples
English Upper Case Letters	A, B, C, ... Z

English Lower Case Letters	a, b, c, ... z
Westernized Arabic Numerals	0, 1, 2, ... 9
Non-alphanumeric characters	.,;:*&%!

It is recommended that the password filter be copied to the primary domain controller for the domain, and to any backup domain controllers. Note that this password filter requires the following registry editing:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
Value: Notification Packages
Type: REG_MULTI_SZ
Data: Passfilt.dll
```

WARNING: Using the registry editor incorrectly can cause serious, system-wide problems that may require you to reinstall Windows NT. Microsoft does not guarantee that any problems resulting from the use of the registry editor can be solved. Use this tool at your own risk.

Restricting Anonymous User Access

Service Pack 3 provides a mechanism for administrators to restrict the ability for anonymous logon users (also known as NULL session connections) to list account names and enumerate share names. Service Pack 3 restricts anonymous logon users from connecting to the registry remotely. A new built-in group, known as Authenticated Users, is created when you install Service Pack 3. The Authenticated Users group is similar to the Everyone group, except that anonymous logon users (or NULL session connections) are never members of the Authenticated Users group.

CryptoAPI 2.0

The Microsoft Cryptography application-programming interface (CryptoAPI) provides developers with cryptographic and certificate functions. The CryptoAPI 2.0 includes the core functionality of the CryptoAPI 1.0 version plus certificate-based functionality. Developers can use Certificates with these public-key operations and perform the necessary encapsulations and encoding to apply certificates within their applications.

TCP/IP Improvements to resist OOB Denial of Service Attacks

An Out of Band Data attack occurs when a user, the receiver of a false URGENT data packet, checks the URGENT POINTER flag to determine where in the segment the urgent data ends. Windows NT then checks the URGENT POINTER to the end of the data frame and no normal data follows, causing the system to hang because it is expecting a normal data flow.

Microsoft has updated module Tcpip.sys within SP3 so that when an Out of Band Data Denial of Service Attacks (OOB) is sent by a user (by setting the URGENT bit flag in the TCP header) that a system stop 0x0000000A does not occur. The service pack and Windows NT 4.0 post-SP3 hot fix address this issue.

Future Direction: Windows NT 5.0

The next major release of Windows NT, version 5.0, will provide additional security features. These features include the implementation of the Microsoft Distributed Security Model that includes the Kerberos authentication protocol, based on the MIT Kerberos protocol, and the Next Generation Directory Services.

Kerberos authentication is used for distributed security within a tree or group of domains, accommodating public and private key security using the same Access Control List (ACL) support model of the underlying Windows NT operating system. The MIT Kerberos V5 authentication protocol is supported with extensions for public key-based authentication in addition to password-based (secret key) authentication.

Directory Services will be linked to the security system, and store information for it, including user accounts, groups, and domains. This will replace the registry account database and will be considered a trusted component within the Local Security Authority (LSA). A single sign-on to the Windows NT domain tree (as exists presently) will allow user access to resources anywhere in the corporate network.

Windows NT Directory Services also support the use of X.509 v3 Public Key Certificates for granting access to resources for subjects (for example, users) that do not have Kerberos credentials. This class of user is most often someone from outside an organization who needs access to resources within the organization. For example, Windows NT Directory Services will allow these certificates to be issued by a trusted authority and be mapped onto Windows NT security groups. Thus, a non-Windows NT user with a certificate can be granted access to resources in the same way as a user with Kerberos credentials.

The following list provides additional information regarding the distributed security model.

- The Directory Service will provide replication and availability of account information to multiple Domain Controllers.
- Directory Services will support a name space for user, group, and machine account information. Accounts may be grouped by Organizational Units rather than the current domain account name space.
- Administrator rights to create and manage user or group accounts can be delegated to the level of Organizational Units.
- Directory Service replication will allow account updates to be made at any Domain Controller and not just the Primary Domain Controller (PDC). Directory Service replicas at other Domain Controllers, formerly BDCs, will be updated automatically.
- The Windows NT Domain Models will change using Directory Service to support a multilevel hierarchy tree of domains. Management of trust relationships between domains will be simplified through tree-wide Kerberos-based transitive trusts throughout the domain tree.
- New authentication protocols based on Kerberos Version 5 and secured using public-

key certificates channels (Secure Sockets Layer 3.0 and Private Communications Technology [PCT] 1.0) become the primary distributed security protocols.

- Common administration tools will be used to manage account information and access control, whether using shared secret authentication or public-key security.
- External users that do not have Windows NT accounts will be able to authenticate using public-key certificates and mapped to an existing Windows NT account.
- The operating system will have integrated support for SmartCard devices.

Conclusion

As shown in the preceding pages, the Windows NT operating system is designed with an architecture that contains many security features and functions. These security features can be implemented in different combinations, depending on the organization’s security objectives and their perceived risk factors. Each successive version of Windows NT has added additional security features. These features, which cover many aspects of security, from user authentication to file and directory access, may be administered and controlled by the systems administrators, are subject to the fixed rules defined by the operating system itself. Methods for reporting on security are also available including event logs, audit reports and performance monitors.

We have attempted to explain the security features of Windows NT in the context of its technical security architecture, as well as the within a general security framework that would be applicable to most organizations. Windows NT is utilized by many businesses and government institutions today in many different production environments protecting a variety of information resources. Since security requirements often differ from organization to organization, and even within organizations, the flexibility of configurable security features enables the ability to implement the desired level of security.

Before deploying Windows NT or any other operating system to support production operations, application development, or networks, governments and businesses need to identify their security risks, establish security policies, and ensure the proper training and supervision of their system managers. Security is a function of sound policies, the appropriate application of technology, and supervision of day-to-day operational practices. Through the use of training, proper documentation, and ongoing security monitoring, a security plan and strategy may be tested for effectiveness on an ongoing basis.

Appendix 1: Security Awareness

Introduction

Security is a combination of technology, policy, and administrative rigor. The overall requirements for security should be based on business risk, technology strategy as well as architecture and application requirements. Computer security needs to be integrated with other practices, such as hiring, training standards, and physical security.

The Importance of Awareness

In addition to having an operating system with extensive security features, the next best security mechanism is an alert administrator who possesses strong security awareness. The system administrator is a key individual, whose duty is to maintain the proper use, performance, and integrity of the systems for which he or she are responsible.

With this said, however, administrators need as much help as they can get in today's environment. This help must include the technology support from hardware and software vendors, financial and authoritative support of their management, and most importantly, the cooperation of the user community.

Hardware and software vendors can help by providing equipment and software designed and produced with security concerns as a top consideration. If physical access to the equipment creates a significant risk, then vendors should include features, such as keyboard and cabinet locks, that provide some degree of tamper resistance. If default passwords are required to install the operating system, then that very same operating system should guide the installer through the password change process before completing the installation. If passwords are the primary authentication mechanism, the software should include some means of ensuring that those passwords are not simple to guess and changed periodically.

Corporate management can help by providing many of the tools and administrative authority needed to run secure systems. Management must clearly understand that good security requires attention, in ways such as proper staffing, training, purchasing needs, and the organizational authority to match the responsibility that their systems and security administrators are assigned. Management is also the primary source of all computer security related policy. They should do their best to produce a policy that is both thorough and realistically attainable. Finally, managers of system administrators should always be aware that some things they ask administrators to do, for purposes of *Making a Deliverable* or *Just to get it working*, may severely reduce the security level of a key system.

The user community can help mainly by cooperating with the security policies created by management and enforced by the systems and security administrators. They can also help by being aware of what other users are doing in regard to systems security. As difficult as it may be, when one user ignores the fact that another user is circumventing security, it poses a risk to all users.

The administrators themselves play the most critical role. When an administrator does something insecure intentionally, or through lack of knowledge, or in following the instructions of their superior, and does not follow-up with proper corrective action as soon as possible, the systems they control may permanently become a security weakness. (It is rarely easy to fix things after a penetration has occurred.)

System administrators should know their systems thoroughly. They should be completely familiar with the normal operating conditions of each of the systems for which they are responsible. This should include full knowledge of the security options for passive and active security monitoring, and the technical procedures they should follow when attempting to isolate a possible problem with a security mechanism. This requires training, diligence, and attention to detail well beyond merely being able to add a new user or perform a weekly backup -- though the process behind these duties should never be minimized. Administrators should also be aware that more than ninety percent of security violations are not from the outside, but from legitimate users who decide to try to exceed their proper authorization.

The Physical Facts

The first line of defense for most computer systems, physical security, is the one that is often in need of attention. This is primarily due to the shift from a central *glass-house* mainframe environment, to today's distributed PC-based environment. In the average office area today, it is fairly common to find a critical application or database server installed in an open room. Couple this with the ease at which someone can gain access to that open room, using social engineering (misrepresenting one's self, lying, or tricking someone into giving a person access), or piggy-backing (following someone through a secure door after they swiped their key card), and the dire situation of most companies becomes apparent.

Good physical security should include not only locked doors around every critical system, but also requires extensive personnel training (e.g., what to look for) and dedicated physical monitoring (e.g., security cameras) to be truly effective.

Bibliography

Cowarts, Robert, Windows NT 4.0 Server-Workstation Unleashed, Sams Publishing, 1997

Custer, Helen, Inside Windows NT, Microsoft Press, 1993

Daily, Sean, Migrating to Windows NT 4.0, Duke Press, 1997

Grant, Glenn, *et. al*., “Troubleshooting with Microsoft: Common Windows NT Problems, Windows NT Magazine,” WWW

Microsoft Corporation, “Windows NT Workstation and Sever,” WWW

Pleas, Keith, “Windows NT 4.0: Explore the New Features,” WWW

Sheldon, Tom, Windows NT Security Handbook, McGraw-Hill, 1997

Ramos, Frank,” Windows NT Security Issues,” Somarsoft Corp., WWW

Coopers & Lybrand, Microsoft, *et. al*., Windows NT 3.5: Guidelines for Security, Audit & Control, Microsoft Press, 1994

Drew Heywood, Inside Windows NT Server (3.51), New Riders, 1995

Karanjit Siyan, Windows NT Server Professional Reference (3.51), New Riders, 1995

___________, Windows NT Server Professional Reference (4.0), New Riders, 1997

Garms, Jason, *et.al*., Windows NT Server 4 Unleashed, Sams Publishing, 1997

Dalton, Wayne, *et. al*., Windows NT Server 4: Security, Troubleshooting, and Optimization, New Riders, 1997

Sutton, Stephen A., Windows NT Security Guide, Trusted Systems, 1997

NT Security FAQ (www.it.kth.se/~rom/ntsec.html)

NT Admin FAQ (www.iftech.com/oltc/admin/admin.stm)

Microsoft Security (www.microsoft.com\security)

NT Security (www.ntsecurity.net)

NT Bugtraq (ntbugtraq.rc.on.ca)