

MSc Information Security 1998/99

IS_4 Computer Security.

***Windows NT Security
Flaws.***

'NT Crackers'

Table Of Contents

ABSTRACT	4
THE GROUP:	4
INTRODUCTION.....	5
WINDOWS NT	5
COMPUTER SECURITY AND WINDOWS NT	5
AIMS & OBJECTIVES	5
LIMITATIONS.....	6
CHAPTER 2. NT ARCHITECTURE	7
NT ARCHITECTURE.....	7
KERNEL.....	7
<i>Processes running in User Mode</i>	8
<i>Processes running in Kernel Mode</i>	8
SERVICES	9
NT FILE SYSTEM (NTFS)	9
WINDOWS NT4.0 REGISTRY	9
<i>What is the Registry?</i>	9
<i>Registry Maintenance.</i>	10
<i>The main Hives.</i>	10
CHAPTER 3. BASIC WINDOWS NT SECURITY.....	11
LOCAL SECURITY AUTHORITY (LSA).....	12
SECURITY REFERENCE MONITOR (SRM).....	12
SECURITY ACCOUNT MANAGER (SAM).....	12
LOGON PROCESS.....	12
USER IDENTITIES AND RIGHTS.....	13
ACCESS CONTROL AND ACCESS CONTROL LISTS (ACL).....	14
DOMAINS AND TRUSTS.....	14
AUDITING.....	15
OTHER SECURITY MEASURES.....	15
CHAPTER 4. NT SECURITY FLAWS.....	16
EARLIER PROBLEMS & FIXES IN NT (SERVICE PACKS).....	16
THREATS CATEGORISED BY LOCATION.....	17
CURRENT THREATS.....	17
UNAUTHORISED DISCLOSURE.....	18
UNAUTHORISED ACCESS.....	25
<i>Exploiting 'system' software</i>	25
<i>Exploiting external services</i>	26
DENIAL OF SERVICE ATTACKS	30
<i>Crashing NT (aka Blue Screening)</i>	30
<i>Other Techniques</i>	33
MISCELLANEOUS THREATS.....	40
<i>NTFS Multiple Data Streams</i>	40
<i>Point-to-Point Tunneling Protocol (PPTP)</i>	40
CHAPTER 5. SECURING WINDOWS NT.....	41
USER ACCOUNTS.....	41
AUDITS.....	42
SERVICES.....	42
THE REGISTRY.....	42
C2 COMPLIANCE.....	43

PHYSICAL SECURITY 43
GENERAL TIPS 43
CHAPTER 6. CONCLUSION..... 44
THE FUTURE OF WINDOWS NT SECURITY 44
APPENDICES 45
APPENDIX A – RECOMMENDED BUG/SECURITY INFO URL LIST..... 45
BIBLIOGRAPHY 46

Abstract

Over recent years Windows NT has become probably the most widely used operating system within the business world. With most systems currently using Version 4.0 and with the impending release of version 2000 this is likely to remain the case for the foreseeable future. Due to the widespread use of Windows NT it is imperative that companies are aware of the security aspects of this operating system as it has a significant impact on their business operations. There remain numerous problems relating to security that Microsoft needs to address in order for companies to feel confident that their Windows NT systems will remain secure.

The group:

Jym Hubbard
Daniel Westwood
Rosemari Wurst
Ralph Gottman
Chris Dickinson
Anna Theodorou
James Clark
Jamie Mcneil
Ebrv Yildiz
Francoise Marie Lima
Ivan Phillips

Introduction

Windows NT

Before we discuss security on the Windows NT platform, we must first ask the question: **What is Windows NT?** Windows NT is a Client/Server network operating system. Windows NT (Windows New Technology) was Microsoft's first 32bit multi-tasking windows operating system. It was developed to supersede LAN Manager, which was Microsoft's networking answer to Novell NetWare.

Computer Security and Windows NT

Computer security is becoming increasingly important and is no longer just the preserve of Governments and Financial sectors. With the advent of the *Internet* the emphasis of security has changed, encompassing not only protecting the server from the client, but also protecting the client from the server. To save resources on the server it now uses applets to run applications from the users hard storage. This starts to deviate from the traditional client server model where the client issued requests to the server, which were processed by the server and the results returned.

The purpose of computer security is to try to provide:

- Confidentiality - Ensure only authorised people can access data.
- Integrity - To ensure that data integrity is preserved and any unauthorised changes can be traced.
- Availability - Enable access to people whom are authorised to use the system.

How does Windows NT fit into this picture? Microsoft products have been criticised for many things, not least for lack of security. With Windows NT, Microsoft hoped to rectify this. Adhering, at least in early releases to the client/server model, Windows NT was first released in 1992 and was evaluated to TCSEC C2 and ITSEC E3 standards with the NT3.51 release. The latest version is Win NT 4 with service pack 4. Version 3.51 was rated C2 under the *DoD Orange Book*¹ standards and it is also possible to make the latest version C2 Compliant.

While Windows NT includes robust security features, NT Server has come under a number of attacks, the success of which has been due primarily to bugs in the operating system, not fundamental architectural flaws. Microsoft's past response to security problems was less than ideal, but Microsoft has made an impressive turnaround over the last year, implementing measures that have established NT as a secure operating system and improved the company's standing. Remaining issues include NT Server's support for the less-secure LAN Manager authentication protocol and the lack of a fully functional directory that provides a common foundation for all security functions.

Windows NT still has room for improvement, for example removing some of the support for less secure architectures, and the removal of well documented bugs from earlier release and service packs, which have still not been fixed.

Aims & Objectives

Chapter 2 aims to give the reader a brief overview of the architecture of Windows NT and describes the four key elements within this design. I.e. the NT kernel, Network Services, NTFS and the registry. Chapter 3 of this document, 'NT Security features' is an overview of the security environment within NT and will describe the NT Security Model. This will also briefly cover the features and services such as the registry, ACL, Accounts, Domains, NTFS etc. These 2 sections prepare the reader for a detailed list of flaws in

¹ See Chapter 5 Securing Windows NT for more information.

Chapter 4 of this document (NT Security Flaws) where we will also highlight several trends of security flaws within NT. These flaws will be roughly categorised according to the CIA model:

- Unauthorised access
- Unauthorised Disclosure
- Denial of Service

Other security flaws, which cannot be placed into any single one of these categories, are labelled Miscellaneous. Each example flaw in these categories will be described as follows:

- Name
- Description
- Vulnerable Systems
- Date first found
- Location (e.g. Kernel, Registry, System Files)
- References

There may be several similar flaws within each category (they may even prey upon the same specific weakness within NT). If so, then this will be commented upon in a summary at the end of each category sub-section. We will attempt to conclude this document by highlighting any trends in the vulnerabilities of NT and comment upon any predicted security problems that may occur to future releases of NT.

Limitations

This document will mainly cover the current version of Windows NT that is in general usage, NT4.0, up to service pack 4. For the purposes of highlighting trends within NT security breaches, some of the flaws outlined in Section 4 will be relevant only to previous versions of NT and, as such, may have been rectified by later versions (or service packs). If this is the case then the version number affected and the recommended actions to be taken to address the problem are detailed. Due to space restrictions Section 4 will only briefly describe a small number of typical bugs within each category. Other bugs within each category will be listed and referenced for further reading.

Chapter 2. NT Architecture

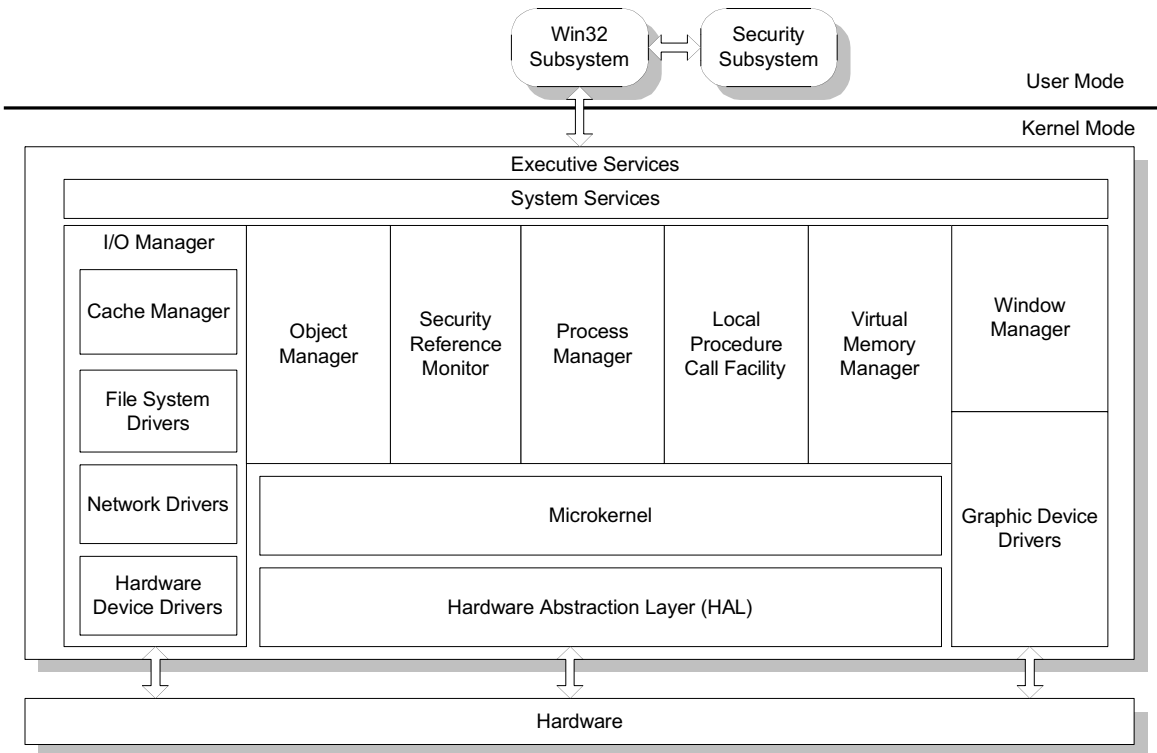
NT Architecture.

This section will briefly describe the architecture of Windows NT to provide a frame of reference for later chapters. Due to the size of the NT architecture it will not be covered in its entirety. The components we will look at are

1. The Kernel
2. The File system.
3. The Registry
4. The Services.

These four components form the backbone of Windows NT server and are also the most likely to be attacked, with the exception of brute force password attacks.

Figure 1: Architecture of Windows NT 4.0



Kernel

The kernel contains all of the processes that enable Windows NT to operate, this includes those processes responsible for security on NT systems. Figure 1 shows the architecture of Windows NT.

The Windows NT processes can be divided into those that have the privilege to run in kernel mode and those that are running in user mode. The kernel mode is a highly privileged mode in which the code has direct access to all hardware and all memory, known as the *Windows NT Executive*. The user mode is a less privileged mode with no direct access to the hardware. Code that is running in user mode can only access its own address space. It uses application program interfaces (API) to request system services.

Processes running in User Mode

Win32 Subsystem:

The Win 32 Subsystem is the native environment subsystem for Windows NT. It includes graphics, windowing and messaging support and the graphics device drivers.

Security Subsystem:

The Security Subsystem consists of Local Security Authority, Security Account Manager and Logon Process. Together with the Security Reference Monitor these components are responsible for the whole security related actions within Windows NT.

Processes running in Kernel Mode

I/O Manager:

The I/O Manager manages all input and output for the operating system. It manages the communications between drivers.

Object Manager:

The Object Manager provides uniform rules for retaining, naming and setting the security of objects.

Security Reference Monitor:

The Security Reference Monitor checks to see if a user has permission to see an object or perform an action.

Process Manager:

The Process Manager creates and deletes processes and tracks process objects and thread objects. It also provides a standard set of services for creating and using threads and processes in a particular subsystem environment.

Local Procedure Call Facility:

The LPC facility is a message passing facility that establishes a client-server connection between an application and an environment subsystem.

Virtual Memory Manager:

The Virtual Memory Manager maps virtual addresses in the process's address space to physical pages in the computer's memory.

Window Manager:

The Window Manager creates the screen interface and is responsible for processes, like messaging, that use window functions without ever affecting the user interface.

Graphic Device Drivers:

Graphic Device Drivers are dynamic link libraries of functions that let the graphics engine communicate with graphic output hardware devices, such as monitors, printers and fax machines.

Micro Kernel:

The micro kernel is the heart of the NT operating system. It schedules threads and handles interrupts and exceptions. The micro kernel can run simultaneously on all processors in a multiprocessor configuration. It synchronises the processes to optimise performance.

Hardware Abstraction Layer

The HAL is a library of hardware manipulation routines that lies at the lowest level of the Windows NT Executive.

Network Services

Windows NT Services enable the outside world and Windows applications to connect to the server and to use its resources, such as disk-space, processor power, printer, programs or documents. Examples of Windows NT services are:

- FTP-server
- WWW-server
- GOFER-server
- TCP/IP printing service
- DHCP-server (Dynamic Host Configuration Protocol)
- WINS-server (Windows Internet Name Service)
- DNS-server (Domain Name Service)
- Support of SNMP (Simple Network Management Protocol)
- RAS (Remote Access Service)
- Services for Macintosh (printer- and file-sharing) (only NT Server)

NT File System (NTFS)

The Windows NT operating system uses the NTFS (NT File System) for storing and retrieving files on a hard disk. When a hard disk is formatted, it is divided into partitions of the total physical hard disk space. Within each partition, the operating system keeps track of all the files that are stored by the operating system. Each file is actually stored on the hard disk in one or more clusters of a predefined uniform size. The NTFS provides a cluster range size from 512 bytes to 64 kilobytes. For any given drive size there is a recommended default cluster size, e.g. a 4 gigabyte drive has a default cluster size of 4 kilobyte. Clusters are indivisible, so for example, the smallest file takes up one cluster and a 4.1-kilobyte file takes up two clusters (8 kilobytes on a 4-kilobyte cluster system). Using NTFS, it is possible to choose the default cluster size, but the larger the hard disk the larger the default cluster size, since it is assumed that a system user will prefer to increase performance (fewer disk accesses) at the expense of some amount of space inefficiency.

After having created a file by using NTFS, a record about the file is created in a special file called Master File Table (MFT). The record is used to locate a file's possibly scattered cluster. NTFS tries to find contiguous storage space that will hold the entire file. Each file contains, besides its data content, a description of its attributes.

Windows NT4.0 Registry

Since Windows 95 Microsoft has, or has attempted to move away from the insecure WIN.INI and other INI files, which were vulnerable both to deliberate and accidental attacks. Despite this Win.ini and System.ini still remain in Windows 9X releases including the new Windows 2000 release, (correct at time of press), this is mainly for compatibility reasons. As the contents of the .INI files were plain text viewable in any ASCII editor, this made them susceptible to tinkering by users wanting to enhance their performance, or perform malicious attacks. For this reason and others, Microsoft sought to protect the system settings and thus developed the *Registry*. The Registry holds all of the system settings for the computer, and is not designed for direct interaction with the user. The registry is normally maintained and access by the Explorer Control Panel and program installations. Microsoft does provide two utilities for direct maintenance of the registry, Regedit.exe and regedt32.exe, but these are for use by system administrators only.

What is the Registry?

The registry is a unified database containing information on the installed hardware, software and system settings. It consists of a series of keys, each with a value arranged in a tree hierarchy. Each set of keys is called a *Hive*. Each key may have sub keys, each of which may again have sub keys etc. At the lowest level of each tree hierarchy there is a value comprising a name, a data type and a value. Possible data types include BINARY (16 Bits), DWORD (4 bytes, displayed in binary, hexadecimal or decimal), SZ (text string), EXPAND_SZ (expandable text string that contains a variable such as % systemroot%), MULTI_SZ (multiple line string; each "line" is separated by a null).

A main file, a save file and a log file back up most of the hive roots. Some hives like LOCAL_MACHINE have no files. CURRENT_USER stores its files in the %systemroot%\Profiles directory.

Registry Maintenance.

Due to the delicate nature of the registry, it is not recommended for users to edit it directly. This is normally left to installation routines and the control panel utilities. However utilities for direct manipulation and searching of the registry are provided. Search programs are provided to enable the user to search for a specific value, which is often useful for diagnosing problems. The provided editors can then be used to change the value. It is however strongly recommended that the registry be backed up first. In the NT Resource kit two utilities are provided to do this. The utilities are as follows:

- **Regedit.exe** - main search facility / program (NB cannot be used to edit the new EXPAND_SZ or MULTI_SZ value types or to implement registry auditing)
- **Regedt32.exe** - used to enter all value types. (NB only searches keys, not values)
- **Regback.exe** - back up Registry.
- **Regrest.exe** - restore Registry.

The main Hives.

HKEY_LOCAL_MACHINE – This contains information about the local machine with the following five (sub) hives:

- HKEY_LOCAL_MACHINE\HARDWARE - Contains hardware, including cards in expansion slots connections through ports, and the related interrupts. This data is determined and stored on boot-up, so it is not saved in any files.
- HKEY_LOCAL_MACHINE\SAM - Security Accounts Manager, containing user account names and passwords and security settings. Maintained on Workstations via User Manager, or on Servers by User Manager for Domains. Files: SAM, *SAM.SAV* and *SAM.LOG*
- HKEY_LOCAL_MACHINE\SECURITY - Contains the security information for the local machine. This is also maintained via User Manager. Files: Security, *SECURITY.SAV* and *SECURITY.LOG*.
- HKEY_LOCAL_MACHINE\SOFTWARE – Stores configurations of loaded applications or packages, under the manufacturer's name. There is also a sub-key called \Classes, which lists all file extensions. Files: software, *SOFTWARE.SAV* and *SOFTWARE.LOG*
- HKEY_LOCAL_MACHINE\SYSTEM - Contains start-up data that cannot be calculated during start-up. This data is stored in ControlSet sub-trees. One of these, CurrentControlSet, is actually a link to one of the others (ControlSet001, ControlSet002, etc.) which contains the data set currently in use. This data is normally modified via utilities in Control Panel. Files: system, *SYSTEM.SAV* and *SYSTEM.LOG*. There is also *SYSTEM.ALT*, which is a backup of the system hive, and makes it possible to undo changes that had unexpected side effects.

HKEY_CLASSES_ROOT - Points to a child (or sub-set) of KEY_LOCAL_MACHINE, at \SOFTWARE\Classes. Contains the Object Linking and Embedding (OLE) and file-class association data.

HKEY_USERS - Contains the user profiles of all users currently loaded on the system. File names: default, *DEFAULT.SAV* and *DEFAULT.LOG*

HKEY_CURRENT_CONFIG - Points to subset of CurrentControlSet, containing the current configuration. It is thus stored in the files called system, *SYSTEM.SAV* and *SYSTEM.LOG* (the same files as for HKEY_LOCAL_MACHINE\System).

HKEY_CURRENT_USER - Points to a child of HKEY_USERS, which is the user who is currently logged on. File names: *NTUSER.DAT* and *NTUSER.DAT.LOG*

HKEY_CURRENT_CONFIG - Points to a subset of CurrentControlSet (as described above), containing the current configuration.

Chapter 3. Basic Windows NT Security.

Unlike other versions of Windows 9X, Windows NT is designed with security in mind. This is not to say that Windows NT is a secure operating system. If used in compliance with the Orange Book C2 security rating then it provides a degree of security but even this is not complete. We can say however that NT provides the capability for basic computer and network security. This is achieved using what we will term the NT Security Architecture. This comprises several components at the system level as well as more conceptual ideas.

The foundation of security in the Windows NT Operating System is the Windows NT security model through which access to any object within the OS is controlled. An object in Windows NT represents a resource; this contains both the data and the functions that manipulate the data. There are three main components which make up this model, the *Local Security Authority (LSA)*, the *Security Account Manager (SAM)*, and the *Security Reference Monitor (SRM)*. This model also includes elements such as logon processing and access control.

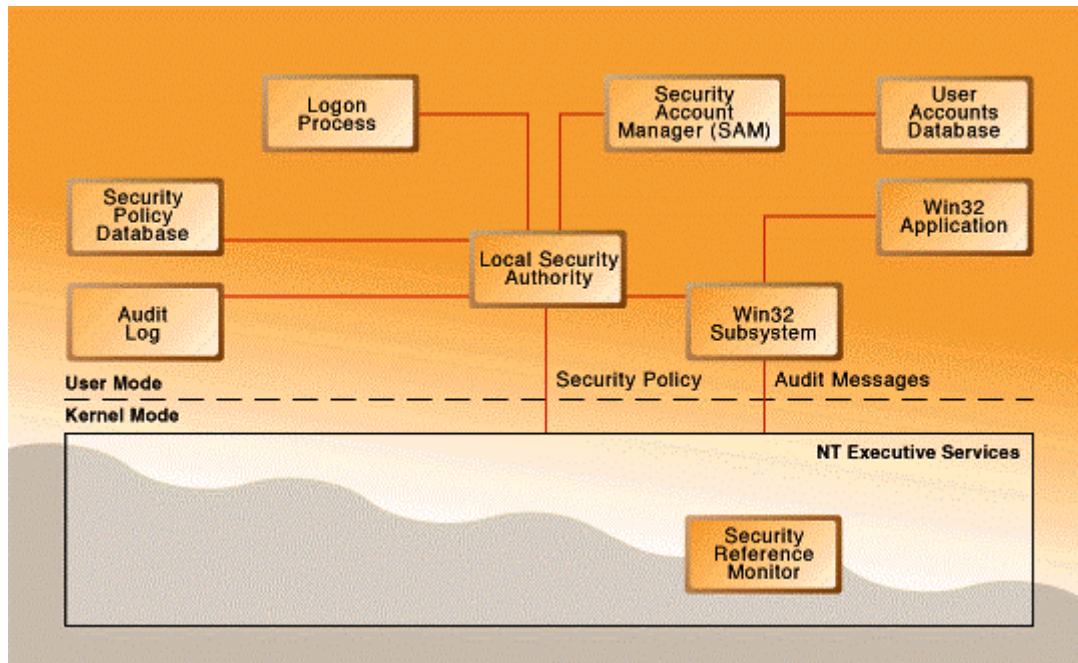


Figure 2. Windows NT Security Components.

Figure 2 shows the main Windows NT security components and their interaction. We will look at each of these services and their interaction and show how together they create the 'secure' backbone of Windows NT. The figure shows a separation between User and Kernel Mode services. This was covered earlier in the document. Suffice to say that Kernel mode services can operate in a privileged mode performing direct access to resources not possible in the user mode. We will now briefly consider each of the three main components in turn.

Local Security Authority (LSA).

The LSA provides validation and authentication of all local and remote logons for all types of accounts within NT. This is done by verifying the logon information with account details, which are stored in the SAM database. It also generates access tokens during the logon process, which are later used to check permissions for any object that the user wishes to access. These access tokens include a Security Identifier (SID), generated by the SAM, for the user and all the groups to which the user belongs. When a user wants to access a particular object, the object permissions are compared with the SID and, if the SID is valid for the object, permission is granted.

Security Reference Monitor (SRM).

The Security Reference Monitor provides services for access validation. The SRM compares the permissions set in each object ACL (Access Control List) with the information in the access token to determine if access should be granted.

Security Account Manager (SAM).

The SAM is a database that contains the user directory. This is kept in the workstation registry for local logins, and the domain controller registry for domain logins. User and Group names, security identities and encrypted local passwords are also contained in the SAM. The registry, which contains the SAM, is not accessible to normal users, and can only be accessed by system processes. These process then use system administration utilities such as User Manager to make the settings available to the Administrators.

Logon Process

In order to log on to a NT system the user must authenticate themselves to the servers, regardless of whether they want to use local or networked resources. In order to do this; the user must invoke the Trusted Path. This is normally achieved in one of two ways.

- 1) Using Ctrl, Alt + Del on a 'restarted' system.
- 2) Selecting Start + Shutdown + Close all programs and Log on as a different user.

Once this has been done the server then has to be provided with an authenticated username and password. This is done using the following process .

1. The user enters a user name and password.
2. The client (NT Workstation) then generates a cryptographic hash of the user's password, and discards the original.
3. The client sends the username in clear text to the server.
4. The server generates a 16byte Nonce (Number used Once) and sends this to the client.
5. The client then encrypts the Nonce with the hash of the user's password.
6. This is then returned to the server. The server then retrieves the hash of the user 's password from the SAM and encrypts the Nonce with it. The two encrypted nonce are then compared and if they match the user is authenticated.

There is another logon process for maintaining LAN manager compatibility.

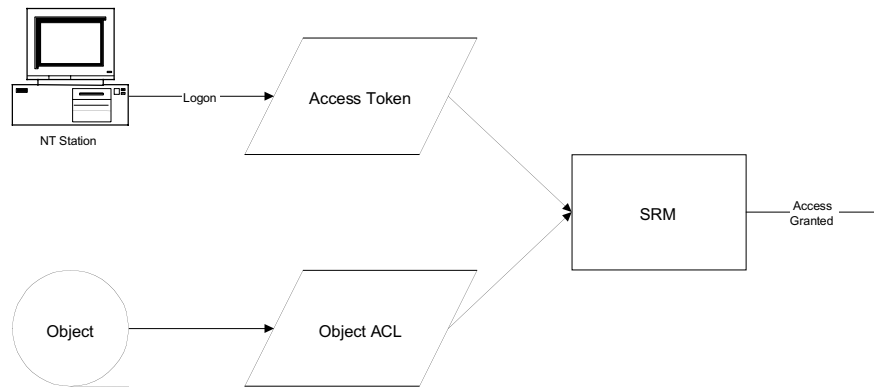


Figure 3. Logon Process for Domain logon.

Briefly the Logon Process for a domain logon is as shown in Figure 3. If the user name is not found on the Local Domain's SAM it is then passed over the network to the Domain Controller for authentication. The benefit of what might appear to be a long and convoluted process is that at no time is the user's password transmitted in the clear. The password is only stored for a very brief time and that is only on the client machine. However the client can still 'prove' to the server that it has knowledge of the user's password and so the server can authenticate the client.

The logon process requires the user to key the Ctrl, Alt and Del sequence at each logon. This protects against most Trojan logon programs, as this sequence cannot be overridden. However this is vulnerable to DOS based Trojan horses booting from removable devices without hardware protection. This could then capture the user's password and then use a fake blue screen to display a false error message requiring a cold reboot.

User Identities and Rights.

Windows NT does not use usernames or password to identify users on a network instead it generates unambiguous numerical identifiers for every user and group of users within the given domain. The *Security Identifier (SID)* consists of a long number, which is generated by hashing the computer name, current system time, and current thread execution time. This enables secure auditing to take place, as even if the system administrator deletes the user group and then recreates them with the same user name, it will be given a new identifier. The new user would also have none of the original user's privileges or access rights, as these would have to be explicitly recreated by the system administrator.

Once a user has been authenticated onto the local domain or network, the LSA generates a security access token for that login session. This token consists of the user's SID and the SID for every group the user belongs to. In addition to the access token the user has a set of rights and privileges granted to the user. These define which objects and resources the user can access and is called the *Security Context*. This is implemented in the Security policy. However as users and programs both have access rights conflicts in access rights may occur. If the user tries to access a program where the program has greater access rights than the user, the security context will be used to ensure that the user does not access anything they should not be able to.

Users may also have system or domain rights in addition to their normal rights. An example of this would be the systems administrator. Examples of the rights include shutting down computers, adding workstations to the domain and creating new users. These rights can overrule the ACL and they can apply to either the local workstation or the entire network domain.

Access Control and Access Control Lists (ACL).

The Windows NT access policy is based upon a set of security principles on which applications are operated. These principles are enacted through NT features and enabling technologies. These principles are; Authentication of a user logging in locally or remotely, Access Control to data based on an identity of a user, System Integrity ensuring that security services can not be tampered with and Auditing records for all security events. The principles are simple, derived from a basic set of threats. Controlling which users may read, write or delete data from databases is at the core of the NT security system.

Provides attachment of specific information to data objects identifying their nature, i.e. user access to the objects and in what manner (read, write, delete, permission changes etc.). Access Control Lists (ACL's) are used in the user environment, they contain a list of NT users or user groups with access permissions to objects that the ACL protects. A user through its ACL may manage an object. In other cases on an administrator may have access to an object ACL, thus restricting user access.

With user authentication Access Control Lists form the cornerstone of Windows NT security. If you remove the ACL you have comparable security to Windows 95. In order to use ACL's NTFS must be implemented. NT works by allowing every object the capability to have an ACL. This then dictates what objects and devices (and ultimately what users) can access each object. Each object may have differing permissions depending on its uses. The typical choice of permission includes:

- Read: Allow the user/ device to read data from the object.
- Write: Allow the user/device to write data to the object.
- Delete: Allow the user/device to delete the object.
- Alter ACL: Allow the user/device to change the Access Control List.
- Make yourself the Owner of the Object. (self-explanatory).

Certain permissions are default. For example the creator of an object is always its object. The owner of an object can always change its ACL. A directory is given a default ACL when it is created which then applies to each file within the directory. This also applies to subdirectories. Another right granted by default by ACL's is "Bypass Traverse Checking". This enables a user to look through a directory tree which they have no permissions to, for an object which they do have ACL rights too. This can constitute a security loophole and it is recommend, for obvious reasons, that this right is removed.

Domains and Trusts.

So far we have only consider the situation where there is a single network domain with a single SAM and backup controller. However due to geographical and political limitations this is usually the exception rather than the rule. Often users from one domain will have to access resources from another domain. In order for this to occur the domains have to be able to trust each other. There are two ways around this,

- 1) Each user has an account on each domain, which will authenticate the user to that domain.
- 2) The user has an account on their main domain and the domain controller will authenticate the user and vouch for the user's security to other domains.

Whilst the first approach may appear to be easier to implement, in the event of the user leaving or having altered access rights it is considerably more difficult to maintain, as well as being more difficult to audit due to different SID on each domain.

In practice the Domain controllers use inter-domain trust and we will now go on to describe some of the mechanics behind inter-domain trust. An NT domain, (Joe) is said to trust another (Jason), when Joe, the *trusting domain*, relies on Jason, the *trusted domain*, to authenticate the users who want to access Joe's resources. The trusted domain provides the trusting domain with the user's security access token. The trusting domain then uses this to determine if the user has the required permissions to access the file, using the files ACL.

In order to set up inter-domain trust, the systems administrators of both domains must be involved. The process is as follows:

- 1) The trusted domain administrator enters the name of the trusting domain and a password.
- 2) The trusting domain administrator then reciprocates by entering the name of the trusted domain and the password.
- 3) This password then provides both domains with a shared secret, which is then used to encrypt communications between them.

Using our example above, this means that Joe trusts Jason to verify that the user who wants to use Joe's resource has been authenticated. However if the user does not have permissions to access the file on Joe's domain, then the user will be unable to access the file. Not only that but the inter-domain trust relationship is one way. This means that while Joe trusts Jason to authenticate the user, Jason does not trust Joe to do the same. Inter-domain trust is also point to point, which means that the trust relationship only extends to the two domains involved and isn't transitive to other servers. I.e. if A trusts B and B trusts C, it does not follow that A trusts C.

There are many models for multiple domain networking on a Windows NT infrastructure.

Auditing.

In order to fulfil the Confidentiality, Integrity and Accountability (CIA) model of computer security, there must be some mechanism for NT to keep track of what a user has done. This is also required for Orange book C2 compliance. In order to achieve this Windows NT has auditing for all security related events built in. The administrator creates an audit policy by checking for either success or failure for a variety of operations. Applications that run under NT can also define their own auditable features that are defined in the registry when the application is installed. Typically features that are auditable are:

- Logons.
- Object access.
- File access.
- Shutdowns/power off and system reboots.
- Changes to security policies.
- Process tracking.

In terms of file and directory auditing, which is only possible with NTFS, the system administrator can specify individual files and directories to audit. This includes which users/groups are to be audited and which of their actions will be audited. Whenever an item is written to the relevant audit log, it will normally contain the following entries:

1. ID of the process that generated the event.
2. ID of the person that attempted to access the process.
3. (optional) A handle ID used to group actions together. E.g. a file open and the file close will have the same handle ID for a given file.

The correct use of the handle ID assists the administrator to identify trends in usage. This can then be used to predict possible attacks to the domain.

Other Security Measures.

Windows NT uses two applications program interfaces, CryptoAPI and the Security Services Provider Interface (SSPI). CryptoAPI provides a way to invoke security services including certificate generation, digital signatures and data encryption. Cryptographic Service Providers provide security services using the Service Provider Interface. Separating the API and the SPI allows applications to make use of the different service implementations with modification. The applications can also use SSPI, which is a higher level interface to use more general security services. E.g. the application can ask SSPI to create a signature without having to specify the individual steps as would be need with CryptoAPI. SSPI is used to establish secure network connections and supports single sign on, it is also used for user authentication for BackOffice.

Chapter 4. NT Security Flaws.

Earlier Problems & Fixes in NT (Service Packs)

When a bug is discovered in NT, Microsoft will release a fix usually termed a 'hot fix'. When there are enough of these fixes Microsoft releases a service pack. As well as containing all the bug fixes for the base installation of NT, whether the base is NT4.0 or NT3.51, each service pack usually introduces some new functionality to the NT system. As each service pack contains all the bug fixes from the base installation there is no need to install previous services packs to a brand new NT4.0 installation, all that is required is to install the current service pack.

The current service pack for NT4.0 is service pack 4 (SP4) while the corresponding pack for NT3.51 is service pack 5. It is widely regarded that NT4.0 SP3 incorporated lots of security fixes for NT and has been dubbed the Security Pack. As well as numerous bug fixes for the kernel especially the TCP/IP stack, SP3 also introduced a version 2 of the Microsoft's CryptoAPI. SP3 also updated the Server Message Block (SMB) authentication protocol, also known as the Common Internet File System (CIFS) file sharing protocol. Mutual authentication and message authentication were introduced to stop various attacks on the SMB authentication protocol. SP3 also introduced a password filter to allow administrators to increase the password strength - from number of characters to the makeup of the password. One other big hole plugged by SP3 was restricting anonymous users connected via null sessions so that they could not access the registry. A new group was added called Authenticated Users of which Anonymous Users are not members and only Authenticated Users can access the registry. The ability to encrypt the registry entries controlled by the Security Accounts Manager was also introduced in Service Pack 3.

In NT4.0 SP4, Microsoft introduced the Security Configuration Manager (SCM) which is an integrated security system allowing administrators to define and apply security configurations across a networked system. The SCM was originally meant to be introduced in NT5, now known as Windows 2000, but as it was finished early it was incorporated into the service pack. SP4 also incorporated security fixes for Microsoft's Point-to-Point Tunnelling Protocol (PPTP) and introduced an enhancement to NT LanMan security protocols. The new LanMan protocol, called NTLMv2, uses better authentication and session security mechanisms to secure communications to older systems such as Windows 98 and Windows for Workgroups while SP4 also introduced an enhancement to the secure channel protocols used by NT workstations to communicate with their domain controller.

While SP4 should have incorporated previous bug fixes there were a few bug fixes that were left out most notably the bugs involving the LSA. (See Microsoft's Knowledge Base articles Q182918 and Q184017) As well as these two bug fixes that were left out of SP4, all new bug fixes appear as 'post SP4 hot fixes' until Service Pack 5 arrives.

Threats categorised by Location.

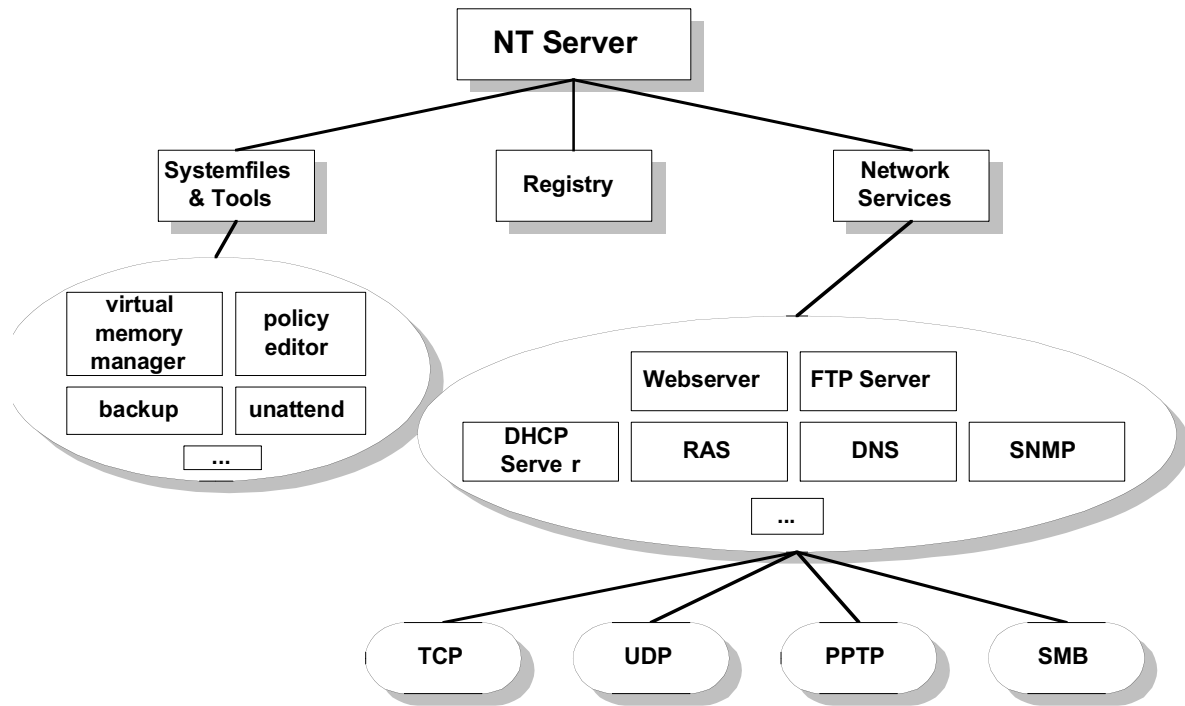


Figure 4: Main locations of Windows NT flaws

In figure 4 it can be seen that the main security flaws that have been found within the NT operating system are mainly concerned with the system-files and tools, the registry and services. Nevertheless there are still several NT flaws that are not within these categories or which are hard to categorise because of the many parts of the system that have to interact to establish these problems.

Current Threats.

After compiling an extensive list of bugs and vulnerabilities in Windows NT the bugs and their associated 'exploits' were grouped into three main threat categories. The first category is Unauthorised Disclosure where an attacker learns information regarding the NT system. The second category is Unauthorised Access which allows an attacker to gain not just disclosure of information but access to read/write to the NT system. Although 'outside' attackers have been mentioned in the first two categories, vulnerabilities which allow legitimate users to gain unauthorised disclosure of information or higher-level access have also been included. The final category is Denial of Service attacks.

In the bug descriptions that follow, a short description is given for each and either Bugtraq, or BugWare makes a reference to the full description of the bug. Bugtraq is a mailing list where all bugs for various operating systems are posted whereas BugWare is a WebSite, which uses various sources to describe bugs (mainly including BugWare). The date field for each bug is the latest version of the bug and the vulnerable

systems field also describes the systems susceptible to the latest version of the bug. Finally, the location of the bug in the overall NT system architecture has been described. Note that in some cases it is difficult to identify the exact location of the bug.

Unauthorised Disclosure

Name: **Account Names**

Description:

A local user can learn all the security ID's for an NT machine and from these can find out the respective account names, domain, and types associated with each ID. If null sessions are allowed to port 139, an attacker can learn this information too.

Vulnerable Systems: NT4

Date:

Location: Kernel

References: Bugware (Admin2)

Name: **Port Binding**

Description:

NT allows any user to bind to any port because it doesn't have the notion of privileged ports. NT also allows users to bind to ports that are already in use and by specifying a source IP to bind to, the user program will take precedence over any NT service.

Vulnerable Systems: NT4 SP3. (SP4 ?)

Date: 6th February, 1998.

Location: Kernel

References: Bugware (Binding), Bugtraq (1998_1/0177).

Name: **Clipboard**

Description:

If you lock a computer, it is still possible to paste the contents of the clipboard onto the username prompt - thus people can find out what you've been editing. Also, if anyone types their password at the logon screen prompt then decides to highlight it, delete it, and walk away it may be possible to view the password in the clipboard.

Vulnerable Systems

Date: 1st April, 1998.

Location: Kernel

References: Bugware (cboard).

Name: CryptoAPI**Description:**

Microsoft uses two file formats to protect users private keys: an old proprietary format used in older versions of IE, and IIS among others, and also the new PFX/PKCS #12 format. Bugs in the design and implementation of these formats allow attackers to learn the private keys of users. In addition, there are bugs in the Microsoft CryptoAPI which allows users to bypass, in some circumstances, all the security protection for private keys. Another problem with the CryptoAPI is the CryptExportKey() function which allows any process with the same user id as the users private key to gain the private key without any further restrictions ! As all ActiveX controls when downloaded from a WebSite run with that user id, it is possible for a remote user to learn the private key of any user.

Vulnerable Systems:**Date:**

Location: Kernel – CryptoAPI.

References: Bugware(CryptoAPI)

Name: Find**Description:**

Although users can be restricted from seeing the find command in the start menu by using the Policy Editor it is possible to start the find command by pressing F3. Also, find allows users to see hidden files, directories, drives, etc and by right clicking on a file you have the same options menu as in explorer. Thus, you can copy USER.DAT to your profile directory and have the rights of the person from whoever you copied the USER.DAT file.

Vulnerable Systems:**Date:**

Location: System Files and Tools.

References: Bugware (find).

Name: 'You are now in France' attack**Description:**

As Win NT must conform to French cryptography regulations the encryption functionality of the CryptoAPI disables itself if the locale is set to France. Conversely, if the locale is changed from France to something else the encryption functionality is enabled. Note that signing and hashing still work when 'in France'.

Vulnerable Systems: All those 'in France' !

Date: 19th May, 1998.

Location: Kernel - CryptoAPI.

References: Bugware (France).

Name: **WS_FTP.INI**

Description:

The file WS_FTP.INI will contain any hostname, username, and passwords that a user has set for automatic entrance to sites. Although the passwords are stored 'encrypted' but it is trivial to decrypt them. File permissions for WS_FTP.INI must be set so that only the owner can read the file otherwise compromise of systems is possible.

Vulnerable Systems: All those systems running WS_FTP client with incorrect file permission set.

Date:

Location: External Application.

References: Bugware (ftpini)

Name: **Web Servers and 8.3 format**

Description:

Some web servers (IIS 4.0, Netscape Enterprise 3.0x, Netscape Fasttrack 3.01, and Website Pro) don't protect files with long names correctly. If a filename is not in 8.3 format then it may be possible to access the canonical name of the file even if the file has access restricted.

Vulnerable Systems: Potentially all systems running web servers.

Date:

Location: Web Servers.

References: Bugware (http34)

Name: **IPC\$ and 'Red Button' attacks**

Description:

Any user can connect to the IPC service using a null id and gain information about the local machine such as user ID lists, group lists, and account names. It might also be possible to modify user information through user mgr for domains. The 'Red-button' attack was thought to be another original attack but, in fact, it is (ref. [rb2]) just using this IPC mechanism.

Vulnerable Systems: NT4 SP2 and below.

Date:

Location: Kernel

References: Bugware (IPC), Bugware (rb), Bugware (rb2).

Name: Microsoft Office Attachments**Description:**

In Microsoft Office (95 and 97) although files can be 'encrypted' any related attachments to 'encrypted' files are not themselves encrypted. This is really an OLE problem but it is still a problem.

Vulnerable Systems: All systems running Microsoft Office '95 and '97.

Date: 7th November, 1997.

Location: External Application.

References: Bugware (mo), Bugtraq (1997)4/0227), breakms.

Name: Linux NTFS**Description:**

As Linux can now read and write to NTFS volumes it is possible to boot from a linux boot disk and read and write to a 'secured' NTFS partition.

Vulnerable Systems: All machines able to boot from floppies without restrictions.

Date:

Location: Physical.

References: Bugware (linuxNTF).

Name: NetBIOS and nbtstat**Description:**

Using a Win95 machine one can use the nbtstat command to gain access to shared directories on Win 95/NT machines. Attack probably possible from Linux as well.

Vulnerable Systems:

Date:

Location: NetBIOS.

References: Bugware (netBIOS).

Name: Ntfsdos.exe

Description:

The NT secured filesystem NTFS can be read from DOS or Win 9x using ntfsdos.exe by booting from a DOS or Win9x boot floppy.

Vulnerable Systems: Machines able to boot from floppies without restriction.

Date:

Location: Physical

References: Bugware (ntfsdos).

Name: Obtaining user listings**Description:**

If someone is running NT server as a domain controller it is possible to obtain a complete user listing, including group memberships of any other NT server on the same network.

Vulnerable Systems: NT4 SP2.

Date:

Location: System files & Tools.

References: Bugware (userlist).

Name: Microsoft Applications and cleartext NT passwords**Description:**

Most network aware Microsoft applications will prompt the user for their password if initial authentication fails and then send it over the network in the clear !

Vulnerable Systems: Most NT machines running Microsoft applications !

Date:

Location: External Applications.

References: Bugware (passwd7).

Name: PKCS#1**Description:**

There is a chosen ciphertext attack against interactive key establishment protocols that use PKCS#1 such as SSL which would allow a sophisticated intruder to recover information about an SSL-encrypted session.

Patches are available for products that are vulnerable.

Vulnerable Systems: Products using PKCS#1 with an interactive key establishment protocol.

Date:

Location: External Applications and also Services running over SSL.

References: Bugware (pkcs).

Name: Plaintext passwords in the Registry

Description: The registry stores some passwords in plaintext.

Vulnerable Systems: Those systems with user readable registries. (should be none !)

Date:

Location: Registry

References: Bugware (reg2).

Name: Downgrade SMB authentication

Description:

As LanManager v2.0 or less sends all authentication (username, password) in the clear then if it could be possible to downgrade authentication if one side doesn't support the more secure protocols. LanManager v2.1 and NT LM 0.12 both send their passwords 'encrypted'. (Okay, these newer protocols don't send passwords at all but the sentiment is the same !)

Vulnerable Systems:

Date:

Location: NetBIOS

References: Bugware (downgrade).

Name: NT4 SP3 TCP Sequence Number predication

Description:

Even by changing TCP sequence numbers every millisecond it has been shown that it is still easy to predict sequence numbers with a sufficient degree of accuracy.

Vulnerable Systems: NT4 SP3. (SP4 ?)

Date: 9th September, 1998.

Location: Kernel.

References: Bugtraq (1998_4/0791)

Summary:

As can be seen from above, there are a number of attacks leading to loss of confidentiality that are due to insufficient password protection. For example, the registry stores some passwords in plaintext while some Microsoft applications send passwords over a network in the clear. Although these flaws do not affect an NT system in them-selves, a user who already has access to the NT system could use them to create further complications, such as denial of service attacks. Another major problem in this category is the use of other file/operating systems to gain access to NTFS filesystem. For example, there are several programs in Dos and Linux (e.g. ntfsdos.exe), that allow a user to boot from a floppy drive (or from another partition), and read and write to the NT partition on that machine. There are no solutions to this type of attack that have been provided by Microsoft so far, the only recommended course of action is not to have dual boot systems and to disable booting a machine from the floppy drive.

Unauthorised Access

Exploiting 'system' software

Name: **\$winnt\$.inf**

Description:

During an unattended installation, the file \$WinNT\$.inf is created in %systemroot%\system32. The file contains all account names and passwords that were created at installation time and the file is not deleted after installation.

Vulnerable Systems: All systems that create workstation accounts during installation.

Date: 25th April, 1998.

Location: System Files & Tools.

References: Bugware (winnt)

Name: **Fragmentation Attacks**

Description:

Using this attack an attacker can bypass a packet filtering firewall and send packets 'directly' to the 'protected' host.

Vulnerable Systems: NT4 SP2 and below.

Date:

Location: Microsofts TCP/IP implementation.

References: Bugware (frag)

Name: **Getadmin exploits**

Description:

There are various programs that allow attackers to gain local admin privileges. By exploiting existing NT services, an application can locate a certain API call in memory, modify the instructions in a running instance, and gain debug-level access to the system, where it then grants the currently logged-in user complete membership of the Admin group. Various API call exploits have been plugged by SP4 but others have been found.

Vulnerable Systems: NT4 SP4, NT5 betas.

Date: 27th July, 1998.

Location: Kernel

References:

BugWare (getadmn5), Bugtraq(1997_3/0030),Bugtraq(1997_3/0033),
Bugtraq(1997_3/0061),Bugtraq(1998_4/0283).

Name: Scheduler Service**Description:**

If a user has physical access to a machine and can rename the scheduler service (atsvc.exe) to something else and then rename the User Manager (musrgr.exe) to 'atsvc.exe' so that the User Manager is loaded instead of the Scheduler service at login then a local user can gain local admin privileges.

Vulnerable Systems: All.

Date:

Location: Physical.

References: BugWare (getadm3)

Name: SAM attacks**Description:**

There are various attacks possible against the SAM including allowing an attacker to masquerade as another user on a remote system due to knowledge gleaned from the SAM and the use of challenge-response authentication in NT. Dictionary attacks against a SAM are possible. SP3 introduced stronger protection for the SAM.

Vulnerable Systems: NT4 SP2 and below.

Date:

Location: Registry.

References: BugWare (sam, sam2, sam3), Re-install password paper.

Exploiting external services**Name: Netbus****Description:**

Similar to the much hyped 'Back Orifice' backdoor for Win9x but NetBus is much more powerful and it runs on NT. Allows an unauthorised user to run privileged operations such as shutting down the computer, open/close CDROM, upload / download any file, get keystrokes, get a screendump, and many more. An attacker must get the remote computer to run a server program.

Vulnerable Systems: NT4 SP4.

Date: August, 1998.

Location: External Application.

References: BugWare (backdoor).

Name: Backup**Description:**

An NT backup tape (or perhaps a recover disk) will have password equivalents that will allow any user to authenticate to an NT server. Note: NT doesn't send passwords over the network it uses a challenge-response protocol and the information in the backup tape will have enough information to allow a user to appear to have knowledge of the password.

Vulnerable Systems: All. (Encrypt your backups !)

Date:

Location: System Files and Tools - backup.

References: BugWare (backup).

Name: Bind**Description:**

Remote root users can poison BIND and Microsoft Windows NT name server caches by forging UDP packets. The name server must have recursion enabled (see reference for details). Could allow an attacker to route all packets from the domain served by the poisoned name server to any site.

Vulnerable Systems: Systems using BIND as their DNS with recursion enabled. NT4 SP3.

Date: 10th April, 1998.

Location: BIND service.

References: BugWare (bind5).

Name: Common Internet File System (CIFS): MITM attack**Description:**

The CIFS is designed to provide accountability and discretionary access control to resources on remote hosts when user level security is used. The protocol NT LM 0.12 (also the LANMAN 2.1 dialect) uses a challenge-response scheme to authenticate the user - unfortunately, it is susceptible to a man-in-the-middle attack.

Vulnerable Systems: All systems using NT LM 0.12 for authentication in CIFS.

Date:

Location: CIFS (SMB).

References: BugWare (cifs, 012).

Name: Common Internet File System (CIFS): Trojan Services**Description:**

The weakness of the NT authentication mechanism for CIFS can be exploited to gain NT user passwords by remote Trojan services. In Unix, Samba can be used to set up such a trojan'ed service.

Vulnerable Systems: NT4 SP4.

Date:

Location: CIFS (SMB).

References: BugWare (cifs2).

Name: NetLogonSAMLogon**Description:**

The contents of the NetLogonSamLogon are unauthenticated resulting in users being able to gain domain admin privileges. Exploit uses Linux transparent proxy filtering with the proxy on the same LAN segment as the server.

Vulnerable Systems: NT4 SP4.

Date: 28th January, 1998.

Location: CIFS(SMB).

References: BugWare (da), Bugtraq (1998_1/0139)

Name: ISAPI scripts and IUSR_MACHINENAME account in IIS**Description:**

It is possible for a ISAPI script to call RevertToSelf() and this changes the script to run as in the all-powerful SYSTEM account.

Vulnerable Systems: Systems running IIS and 'untrusted' ISAPI scripts.

Date:

Location: Services - IIS.

References: BugWare (rev).

Name: Routing and RSA filtering problems**Description:**

It is possible to connect to ports that have been thought to be filtered.

Vulnerable Systems: Systems running RRAS 1.0.

Date: 27th June, 1997.

Location: Services - RRAS.

References: BugWare (ras), Bugtraq(1997_2/0060).

Name: SMB Connection Hijacking and others**Description:**

It is possible to hijack a SMB connection but it requires a combination of sequence attack and UID/TID spoofing. Another attack (ref.: SMB2) was possible but has been fixed with SP4.

Vulnerable Systems: NT4 SP4.

Date: 6th February, 1998.

Location: SMB

References: BugWare (smb, smb2), Bugtraq (1998_1/0174).

Name: Quake, Quake2, Quakeworld**Description:**

The IDsoft developers put a backdoor into Quake 1, Quake 2, QuakeWorld, Quake 2 Linux and Quake 2 Solaris so that they could access servers during testing. When spoofing their IP address allows remote users to run arbitrary commands on server machine.

Vulnerable Systems: All systems running the Quake variations.

Date: 1st May, 1998.

Location: External Application.

References: Bugtraq(1998_2/0216).

Name: Bypassing Proxy Server packet filters**Description:**

By disguising service-specific commands as HTTP headers it is possible to bypass packet filtering.

Vulnerable Systems: All running Microsoft Proxy Server 2.0

Date: 8th October, 1998.

Location: Services - Proxy Server.

References: Bugtraq (1998_4/0043).

Denial of Service attacks

Crashing NT (aka Blue Screening)

Name: **NT File Caching Algorithm**

Description:

There was a nasty bug in NT's virtual memory manager that causes all available memory to be irrecoverable lost every time the system fails to grow the page file (either because it runs out of disk space or because the configured maximum size has been reached).

Vulnerable Systems:

Date: 7th November, 1997.

Location: System files & tools - virtual memory manager.

References: BugWare (cache).

Name: **Domain_Create_Alias**

Description:

Allows any user to create local groups on the domain controller so if an attacker creates lots of groups then he can make the SAM huge and crash the server. The administrator can disable Domain_Create_Alias in the registry but at a loss of functionality.

Vulnerable Systems:

Date:

Location:

Registry.

References: BugWare (dca).

Name: **IP Fragment overlap (aka Teardrop)**

Description:

All WinNT machines with service packs up to SP3 are vulnerable to an IP fragmentation attack which will crash the machine. Only 10 to 15 fragmented IP packets are required to crash the machine. Fixed in SP4. There are many variants of this initial problem including ipfrag2, ipfrag3, ipfrag4, ipfrag5 as shown in the References:. There is a new variation of the IP fragmentation overlap attack that is not fixed by SP4 shown as ipfrag6 below.

Vulnerable Systems: NT4 SP3.

Date:

Location: Kernel.

References: BugWare (ipfrag, ipfrag2, ipfrag3, ipfrag4, ipfrag5, ipfrag6).

Name: **Bug in NtAddAtom**

Description:

There is a bug in NtAddAtom which allows a trivial program to crash NT.

Vulnerable Systems: NT4 SP3.

Date:

Location: Kernel.

References: BugWare (ntcrash).

Name: **Out of Band attacks**

Description:

There were various attacks using out of band signaling in TCP causing NT to crash.

Vulnerable Systems: NT4 SP3.

Date:

Location: Kernel.

References: BugWare (oob3).

Name: **Ping of Death**

Description:

By sending large ICMP packets from NT it is possible to corrupt the local TCP/IP stack. Fixed in SP3. A variation (ref: ping4) of this attack will lock the machine, again, the service pack will fix this. There are at least two (ref: ping5, ping6) other variations which allow a user to crash or lock a remote NT machine.

Vulnerable Systems: NT4 SP3.

Date:

Location: Kernel.

References: BugWare (ping, ping4, ping5, ping6).

Name: **NT RAS PPTP**

Description:

By sending a pptp start session request with an invalid packet length in the pptp packet header it is possible to crash an NT machine.

Vulnerable Systems: NT4 SP3, with RRAS 1.0

Date:

Location: Services - RRAS.

References: BugWare (rasppt)

Name: **Smbclient and long messages**

Description:

It is possible to crash NT RPC by sending a message with a very long user id.

Vulnerable Systems: NT4 SP2.

Date:

Location: SMB.

References: BugWare (smbc).

Name: **SMB Logon packet**

Description:

Due to incorrect processing of an SMB logon packet it is possible to corrupt the memory of the NT kernel resulting in a system crash.

Vulnerable Systems: NT4 SP3.

Date:

Location: SMB.

References: BugWare (smbc2).

Name: **Linux and smbmount**

Description:

It is possible to crash WinNT using an incorrect version of smbmount from linux.

Vulnerable Systems: NT4 SP2. (Although NT3.51 immune)

Date:

Location: SMB.

References: BugWare (smbmount)

Name: **TCPIP.SYS**

Description:

It is possible for a user to crash the local system by calling the undocumented function NtDeviceIoControlFile with a handle to TCP/IP and the 'correct' parameters.

Vulnerable Systems: NT4 SP4.

Date: 28th September, 1998.

Location: Kernel.

References: BugWare (tcpip7)

Name: **NT Floppy driver**

Description:

Trying to access a linux bootdisk or any other non-standard disk results in an instant blue screen.

Vulnerable Systems: NT4 SP4.

Date: 16th September, 1998.

Location: Kernel.

References: Bugtraq (1998_3/0837).

Other Techniques

Name: **Chargen port**

Description:

A simple denial of service attack is make several connections to the chargen port. The chargen port is used to test terminal setups by sending all the printable characters over and over again. See ref:tcpip2 for another variation on this attack.

Vulnerable Systems: NT4 SP?

Date: 24th July, 1997.

Location: SimpleTCP services - chargen.

References: BugWare (chargen2, tcpip2), Bugtraq (1997_3/0152).

Name: **Various CPU utilisation attacks**

Description:

By telnetting to the NT localhost, it is possible to make the CPU utilisation rise. Vulnerable ports include 1038 (TPSVCS.EXE), 1043 or 1091 (WINS.EXE), 1029 (DNS.EXE), 1031 or 1033 or 1035 (INETINFO.EXE). Some other services (eg. CSM proxy on ftp port) are exploitable remotely.

Vulnerable Systems: NT4 SP?

Date: 28th February, 1998.

Location: Kernel and services.

References: BugWare (cpu2).

Name: **DHCP logging**

Description:

If the log file becomes too big the DHCP server will crash. DHCP logging was introduced in NT4 SP3.

Vulnerable Systems: NT4 SP3.

Date: 25th January, 1998.

Location: Services - DHCP server.

References: BugWare (dhcp)

Name: **Delete and file access**

Description:

If a file has read-only access for Everyone then any user can delete the file even though Everyone doesn't have delete permissions.

Vulnerable Systems: NT4 SP4.

Date:

Location: Kernel.

References: BugWare (del1).

Name: **DNS and AnswerCount**

Description:

If a DNS query is modified so that the original query's AnswerCount field is greater than 0, the DNS server may cause an access violation and stop.

Vulnerable Systems: NT4 SP2.

Date:

Location: Services - DNS Server.

References: BugWare (dns)

Name: DNS cache poisoning**Description:**

An attacker can poison the DNS cache of a DNS server which is configured to respond 'recursively'. The DNS server uses predictable sequence ids for queries which an attacker can use although the DNS server has recently been upgraded to use random sequence ids making it more difficult for the attacker to guess ids.

Vulnerable Systems: NT4 SP3. (SP4 introduces random sequence ids)

Date:

Location: Services - DNS server

References: BugWare (dns2)

Name: Killing DNS Server**Description:**

By sending lots of garbage to the DNS service port the DNS server will crash with an access violation.

Vulnerable Systems: NT4 SP3.

Date:

Location: Services - DNS server

References: BugWare (ns)

Name: Site Server and Verifone vPOS**Description:**

If logging is enabled then it is possible to generate lots of logs and fill the hard drive. Also, the vPOS service cannot be started automatically after a crash. Finally, a lot of registry entries must be created to allow vPOS to work with Microsoft Site Server.

Vulnerable Systems: Systems running evaluation version of vPOS with Microsoft Site Server.

Date:

Location: Services - Site server with vPOS.

References: BugWare (verifone)

Name: Locking files**Description:**

A trivial program has been written which will deny access to any file that a user has read access to.

Vulnerable Systems:**Date:****Location:** Kernel

References: BugWare (lock)

Name: Lsass.exe**Description:**

The LSA can only handle 2048 open SAMR pipes any further connections are not allowed. Also, if garbage is written to one of the opened pipes lsass.exe will start eating all available memory. Note that we can open these pipes through a null session.

Vulnerable Systems: NT4 SP2, and now NT4 SP4.

Date: 26th October, 1998.

Location: Kernel.

References: BugWare (lsass), Bugtraq (1998_4/0212).

Name: Memory leak in netstat.exe**Description:**

There is a memory leak in netstat.exe when connections are finished the memory used for the connection table is not freed.

Vulnerable Systems:**Date:**

Location: System files and tools - netstat.exe

References: BugWare (netstat)

Name: Rollback.exe**Description:**

This program wipes out all registry entries and forces a reinstall of NT. This program is included with WinNT. Trojans are possible by renaming rollback.exe to something like 'ie.exe'. If an attacker can run programs remotely then a reinstall will be necessary (ref: rollback2).

Vulnerable Systems:**Date:**

Location: System files and tools - rollback.exe

References: BugWare (rollback, rollback2).

Name: TCP/IP invalid packets**Description:**

It is possible to stop the server from accepting any data from the network by sending a carefully crafted packet. (Has invalid sequence number, invalid window size announcement, Urgent, FIN, and RST flags set; plus a few other properties)

Vulnerable Systems:**Date:**

Location: Kernel.

References: BugWare (tcip).

Name: Schedule Service**Description:**

There is a bug in the AT command of the schedule service that will schedule lots of jobs if a hyphen is placed in the AT command line. On VAX/DCL, a hyphen is used as a line continuation character.

Vulnerable Systems:**Date:**

Location: Services - Schedule.

References: BugWare (schedule).

Name: **scopy**

Description:

It is possible to change the ACL of C:\winnt to only allow access to a single user. Problems occur due to a . (dot) being placed as the destination of an scopy command.

Vulnerable Systems:

Date:

Location: System files and tools - scopy.exe

References: BugWare (scopy)

Name: **Snork Attack**

Description:

Allows an attacker with minimal resources to cause a remote NT system to consume 100% CPU cycles by exploiting WinNT RPC service.

Vulnerable Systems: NT4 SP4.

Date: 29th September, 1998.

Location: Services - RPC services.

References: BugWare (snork)

Name: **SYN flooding**

Description:

Allows an attacker to tie up all (or some) of the ports on TPC/IP-based services.

Vulnerable Systems:

Date:

Location: Services - TCP/IP based.

References: BugWare (synnt)

Name: NT Systemcalls**Description:**

Due to the way system calls are implemented it is possible for various denial of service attacks. It is also possible to use bugs to gain higher level access.

Vulnerable Systems:

Date: 19th October, 1997.

Location: Kernel.

References: BugWare (syscalls), Bugtraq(1997_4/0093).

Name: Windows Internet Name Service (WINS) Server**Description:**

It is possible to flood a WINS server by sending UDP 13 packets to it resulting in the server stopping normally. SP4 fixes the problem. Other related (ref: wins2) problems are fixed with this service pack.

Vulnerable Systems: NT4 SP3.

Date:

Location: Services - WINS Server.

References: BugWare (wins, wins2).

Name: 'Land' attack**Description:**

By sending a spoofed packet with host and port address the same as the intended recipient and if the SYN flag is also set then it is possible to lock the machine. Another variation works 'well' against NT4 SP3.

Vulnerable System: NT4 SP3.

Date:

Location: Kernel.

References: BugWare (tcpip5, tcpip6).

Name: Reseting Network connections**Description:**

A bug exists in Microsoft's implementation of TCP/IP where an attacker can reset existing connections as long as he can work out the TCP port number and IP address of both ends of the connection.

Vulnerable System: NT4 SP4.

Date: 6th October, 1998.

Location: Kernel.

References: BugWare (tcpip8).

Name: **Microsoft Proxy Server 2.0**

Description:

In some instances if a client connection to the proxy server is aborted the connection the proxy server has made to the remote server is not RESET. A simple DOS attack is then to get the proxy server to connect to the chargen service and abort the client connection.

Vulnerable System: NT4 SP3 with Microsoft Proxy Server 2.0 running.

Date: 9th October, 1998.

Location: Services - Proxy Server 2.0

References: Bugtraq (1998_4/0059).

Miscellaneous Threats

NTFS Multiple Data Streams

It is possible to 'hide' data within the file structure of NTFS by using multiple data streams, sometimes called alternate data streams. Also, from Bugtraq (1998-0099), the command-line ftp program 'understands' multiple streams and allows their upload/download.

Point-to-Point Tunnelling Protocol (PPTP)

Bruce Schneier and Mudge have published a paper describing various problems with Microsoft's Point-to-Point Tunnelling protocol. (PPTP). Microsoft has claimed that SP4 will fix all of the issues raised but there are still a few question marks. Aleph One has also posted more problems with PPTP. There is also a denial of service attack posted to bugtraq.

Chapter 5. Securing Windows NT.

After chronicling all that is wrong with Windows NT it would be unfair to finish this document without a discussion on how Windows NT can be made more resistant to attacks. Notice the use of the word resistant as opposed to *secure*. Whilst Windows NT has been rated to C2 levels this is only on an un-networked implementation. We will cover the C2 security standard briefly, later in this chapter.

Most NT attacks consist of one of the following:

- Password Cracking
- Remote Registry Access.
- CGI or ASP programs on web servers.

User Accounts.

Before user accounts are created a secure account policy should be established. In order to do this the system administrator should use the Account Policy dialog box, which is in the Domain User Manager. This can be used to configure settings such as:

- Number of bad passwords before the account is locked out.
- Length of time the account is locked for.
- How long passwords are valid for.
- Password Uniqueness

Correct usage of these settings can help prevent Brute force attacks using automaton. Most people still use insecure passwords, including the names of their loved ones, pets and dates of birth. These are easy for programs to hack into or for intruders to guess. There are also available programs that will run through dictionaries of common passwords. In order to make password attacks more difficult, the network should enforce a minimum of 8 characters for a password and enforce password changing and uniqueness. Password changing forces a user to change their password at an interval set by the system administrator, and uniqueness prevents lazy users from using the same old password every time. Password filters such as *Passfilt.dll* should be used.

For advanced protection of passwords, one has to note that NT stores two versions of the user's password, The LANMAN hash and the NT Hash. The LANMAN version is encrypted in such a way that enables hackers to use tools such as *L0phtCrack* to recover the 8th to 13th characters of the password. In order to protect this extended characters and punctuation should be used. This makes brute force attacks on the passwords significantly more complex. This can be supplemented by using token-based authentication from a third party package.

Another major source of weakness is the default user groups, which are built into Windows NT. This includes the default Administrators account. The best form of defence against attacks on the default administrators account is to simply disable it whilst leaving it in place. If the account is left in place then the attack can find this out. If the account is disabled, the attacker will have to spend the time to brute force the password before he discovers this fact. In order to disable the account – create the new administrator account and duplicate all the administrator account policies and permissions and then remove them from the administrator's account.

Another common security weakness occurs when users leave companies or change their position within the company. User accounts are either left inactive or the users end up with permissions that aren't consummate with their new positions. However the deletion of accounts can cause problems, as there are only a limited number of SIDs available, and the list of SIDs is not cleared until the NT Server is reinstalled. In order to overcome this user accounts should be renamed and disabled.

The largest weakness here is the Guest account. There is much (heated) discussion about whether Guest accounts should be allowed or indeed are useful which we won't enter into here. The best way to prevent security breaches through the guest account is to delete it or otherwise disable it until needed. A check should be made that it remains disabled.

Users should also be discouraged from leaving workstations unsecured, even if only for a minute, and at the end of the day machines should be powered off.

Audits.

For more information on auditing see chapter 3. However as a general rule, it is a good idea to audit as many features as possible.

Services.

Windows NT can be greatly enhanced by installing additional services. However these services if not correctly configured can be one of its biggest downfalls. The main reason for this is that a service requires a user account to run under. This account then determines the level of security afforded to the service. To secure your services against attack try the following:

- Do not use domain accounts for services. This is because any one on the administrator group can then find out the name and password of the account the service is running under.
- Run only the services required for a particular machine to be functional. Disabling service such as messenger and alerter, help to secure the station against remote attacks.

One problem with services is that when they install they usually default to the system account. This means they have the same level of access as the OS itself. This leaves a large potential for problems, especially as the majority of services require this high level of access to function, and to revoke it in order to replace it with a lower level may cause system malfunctions. Some services enable you to choose the account they run under. A process of trial and error is then needed to determine the acceptable minimum level of security for the service. Services themselves must be watched to ensure that they do not generate any security holes that can then be exploited. In order to do this the systems administrator must stay current with vendor websites and service packs.

When a service is installed, the account it is installed under should be examined, using the network control program in Control Panel. The service should be checked to see if it runs under the system account or not. If it doesn't the user account should be checked to ensure that it has permissions to run the service.

The Registry.

This is probably one of the biggest areas of attack on an NT platform. This is because NT stores so much of its security information in the Registry or related files, and then tries to protect access of the registry. This means that if an unauthorised user gets access to the registry they have the potential to do large amounts of damage.

Proof of this is in the fact that most books that discuss NT security dedicate separate chapters to the protection of the registry. One problem in securing the registry is that NT does not just store the registry in two files. It uses a whole batch of files stored in different locations. This means that the system administrator has to make sure that all of the files are properly secured.

Securing the Registry is a complex job and would take too long for us to cover it in-depth. We will however briefly look at steps that can be taken to help prevent an attack.

- The simplest way to prevent the registry from simple attacks is to prevent access to the registry editor.

- Restrict access to the registry to administrators only.
- Ensure that only people who REALLY need it have administrator privileges.
- Remove permission to the Regedit and other registry utilities from all but the administrators group.
- Change the user permissions for the user profiles by locating the User hive in %system folder%\Profiles\%username%.
- Change ACL for keys and sub-keys. These can be altered using Regedt32. However this is not recommended – except for software installed by system administrator. Incorrect tampering with this can cause NT to fail to load.
- Audit registry access.

Note: do not modify any other hives as these are managed automatically and changing them will cause NT to crash.

More information on securing the registry can be found on the Microsoft web site. However great care should be taken and backups of the registry should be made.

C2 Compliance

A document on NT security would not be complete without some mention of C2 compliance. What is C2? It is a security level rating from the Orange book standard of Department of Defence. It is described by the DoD as:

“C2 is a level of security defined by the department of defence as a baseline measurement of a secure operating system. Today network operating systems are used to share key information and resources among many users throughout organisation of various sizes. Frequently the information stored on network servers is meant to be secure and is intended for use only by authorised individuals. The ability of these networks to prevent unauthorised access to information is of paramount concern to the security and competitiveness of an organisation.”

Microsoft worked closely with the Department of defence to ensure that Windows NT was C2 compliant. However the common mistake is to install Windows NT out of the box and expect to have a C2 compliant system. This does not happen, as other configurations are almost always required.

The complete requirements for C2 security can be found in the publication Trusted Computer System Evaluation criteria more commonly known as the Orange book. This is published by the National Computer Security Center. These are available on the Internet. There is also the Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria otherwise known as the Red Book.

Physical Security.

Whilst securing the server from remote attacks and protecting user accounts from brute force attacks is laudable, it is also recommended to secure the server physically to prevent physical attacks to the server itself. Physical security can range from a sturdy lock on the server room door to the use of biometrics.

Keeping the server in a clean well ventilated room with a sturdy lock and clean air supply will not only help with the security but will also help prevent server crashes due to accidental damage.

General Tips

- Minimise trust relationships between workstations and domains. Use different passwords on different machines for a given name. Explain to the users that shared passwords compromises security.
- If remote administration is used, ensure that you are running SP3 and require SMB message signing, to protect message authentication and integrity.
- Use the latest version of Service Packs, as each version will fix more security bugs.

Chapter 6. Conclusion

The Future of Windows NT Security

NT Server and Workstation form a good foundation for building network security. While present shortcomings in NT's directory place constraints on scalability and manageability, the general NT Security Architecture is good and Microsoft is dealing with security problems at a rapid pace.

Very soon the first commercial version of NT 5.0/Win2000 will be released, which will include a new generation of Internet functionality. The server will support a larger memory capacity for 64-bit processors, encrypted file systems, and Internet security technology based on public-key cryptography across public networks. However, it should be made clear that no network deployment is truly secure without careful thought about the implementation details. Network administrators should inspect their systems frequently, and plan with future threats and future capabilities in mind. They should be getting ready for Win2000 now. To do this they should be reading all the relevant "coming future enhancements", which include the new Directory Services, Smart cards, Identity mapping (X500 to NT SIDs), Kerberos public-key authentication, SSL, IPSec, PPTP, Certificates and Crypto API.

Looking even beyond the upcoming version 5.0, it can be seen that Windows NT domains, with their one-step trust relationships, suffer by comparison to other systems in large environments. So, this will be improved. Many alternative authentication cryptosystems will turn up, like Kerberos, now that the U.S. government relented slightly on its 40-bit key export restrictions. ACLs won't change much, but more sophisticated audit and analysis tools will always be in need.

However, the Trojan Horse threat is now worse than ever. Increased security in Windows NT depends on its ability to limit the capabilities that "*malicious programs*" gain, regardless of who runs them. Talking about future plans, the fact that COM+ will be bundled with Windows NT 5.0, guaranteeing middleware technology for a commodity price, clearly enhances Microsoft's chances in its endless pursuit to capture the server market for multi-tier enterprise applications. Also, a range of new technologies is due to come on-stream before and during 2000, so expect the unexpected.

The bottom line is that security is there to use or lose. Windows NT is a good start and will become a lot better in the near future, but it's up to the system administrator to plan a secure network environment and ensure that s/he is up-to-date with the latest technologies.

Appendices

Appendix A – Recommended Bug/Security Info URL List

Bugtraq Mailing List Archives: <http://geek-girl.com/bugtraq/index.html>

Bugware Site: <http://oliver.efri.hr/~crv>

<http://www.ntshop.net/>

A good site for recent bugs and fixes.

http://www.iss.net/cgi-bin/xforce/xforce_index.pl

A good site for bugs and suggested fixes on any platform.

Good layout, also stating risk levels of each bug.

<http://www.ntsecurity.com/News/index.html#ntsites>

Good site for other Security links.

<http://www.microsoft.com/ntserver/nts351/ttsecur.htm>

Slow to start up and rather biased.

<http://www.securityserver.com/>

Good site for overall security issues and contains many links.

Badly laid out and confusing to navigate through.

<http://www.winntmag.com/magazine/Article.cfm?issueid=56&articleid=3671>

Windows NT Vulnerabilities and Defences

<http://www.ntbugtraq.com>

A mailing list and discussion groups for security and security bugs in NT

Bibliography

Author(s) M. Kelley, W. Mayson

Title Windows NT Network Security: A Managers Guide

Date December 1997

Author(s) Steve Sutton

Title Microsoft Product Security: An Overview

Date September 1997

Author(s) Microsoft Inc.

Title Final Evaluation Report: NT Workstation and Server V3.5 + U.S. SP3

Date April 1996

Author(s) Lance Jenson, John Sankey

Title Windows NT4.0 Registry

Date October 1998

Author(s) NeonSurge

Title WindowsNT Registry Overview

Date

Author(s) NeonSurge

Title Understanding SMB's and Components

Date

Author(s) Microsoft Corporation

Title Basics and Installation Windows NT Server Version 4

Date 1996

Author(s)

Title Maximum Security : A Hacker's Guide to Protecting Your Internet Site and Network

Date