

Windows NT Security
CS384 - Term Paper

Submitted to: Dr. Taylor
Submitted On: 2/3/2003
Submitted By: Ben Sevener

<u>Table of Contents</u>	<u>Page #</u>
<u>Introduction</u>	3
Description of Security	
- Accidental or Intentional?	4
- operating system threats	7
- program threats	7
- system threats	8
Windows NT Security	
- Overview	10
- User Accounts	11
- Security Subsystem	13
- Objects and Permissions	15
- Virus Protection	18
<u>Conclusion</u>	19
<u>Bibliography</u>	20

Introduction

With the use of computers in today's society, the last thing one would need is a virus, bug or any other sort of intentional breach into his or her computer. Recently, a website published the statistics for the Sapphire/Slammer SQL worm and told of its effects unto society.

- "This worm required roughly 10 minutes to spread worldwide making it **by far the fastest worm to date.**"
- "In the early stages [the number of compromised hosts] was doubling in size every 8.5 seconds."
- "At its peak, achieved approximately 3 minutes after it was released, Sapphire scanned the net at over 55 million IP addresses per second."
- "It infected at least 75,000 victims and probably considerably more."

(<http://www.securitystats.com/virusstats.asp>, 2000)

Absolute protection of the system from intentional abuse is not possible, but the cost to the perpetrator can be made sufficiently high to deter most, if not all, unauthorized attempts to access the information within the system. In order to protect against these and other attacks, security measures must be taken at four different levels, physical, human, network and operating system.

Protection at the physical level involves the site or sites containing the computer systems being physically secured against armed or secret entry by intruders.

With the human level, users must be screened carefully to reduce the chance of authorizing a user who then gives access to an intruder. This may happen in exchange for a bribe for example.

At the network level, most of computer data in modern systems travels over private leased lines, shared lines like the Internet, or dial-up lines. Interception of this data could be just as disastrous as the break-in of a computer. Interruption of these communications could be a remote denial-of-service attack and reduce the use of and trust of the system.

Finally, the operating system must protect itself from accidental or purposeful security breaches. This paper will highlight some of the aspects of Windows NT operating system security.

Description of Security

Accidental or Intentional?

Security breaches can be categorized into two main types: accidental or intentional (malicious). Accidental misuse is much easier to protect against than malicious misuse. Some of the forms of malicious misuse are Social Engineering, Dumpster Diving, War Dialing, and Denial of Service attacks. (Olsen, Loughran, 2002)

In social engineering, a hacker may use tricks and disinformation to gain access to private, sensitive information. For example, suppose a group

of high school students want to gain access to a local business's computer network. They then create a form that asks for what appears to be innocent and harmless information, such as the names of all the secretaries and executives and their spouses, as well as the names of children, pets, and so forth. The students-turned hackers say that this simple survey form is part of a social studies project. Using this form, the students are able to quickly penetrate the system due to most of the people on the network are using the names of pets and spouses for their passwords. (Stanger, Lane, Crothers, 2002)

If you've ever written down a password or access code, memorized it, and then thrown it away, you are subject to Dumpster Diving. If you are a security administrator, network supervisor or any other individual who holds important information, you better believe someone is digging through your trash to obtain this information. Many systems are broken into using this method of attack.

A war dialer is a tool for attackers to dial numbers in a sequential order and wait for one to answer that allows access into your network. Attackers, security assessment teams trying to get into your system frequently use this tool.

A denial of service (DoS) attack is when a normal user, organization or client is denied access to information they normally would have. This loss of service can affect your email, network or any other resource available on the network. Suppose that your company has a website that millions access each day. What would happen to your company if they could not access your site? Instead, they might switch over to another site or provider of your particular service. If a denial-of-service attack is perpetrated with enough force and consistency, it can corrupt applications and files, requiring them to be reinstalled. DoS attacks are usually intentional, malicious and are usually meant to shut down your business. One thing to be careful of is that you don't cause an unintentional DoS attack on your own organization by blocking access to the needed ports.

Refer to Figure 1-1 for a description of a DoS attack.

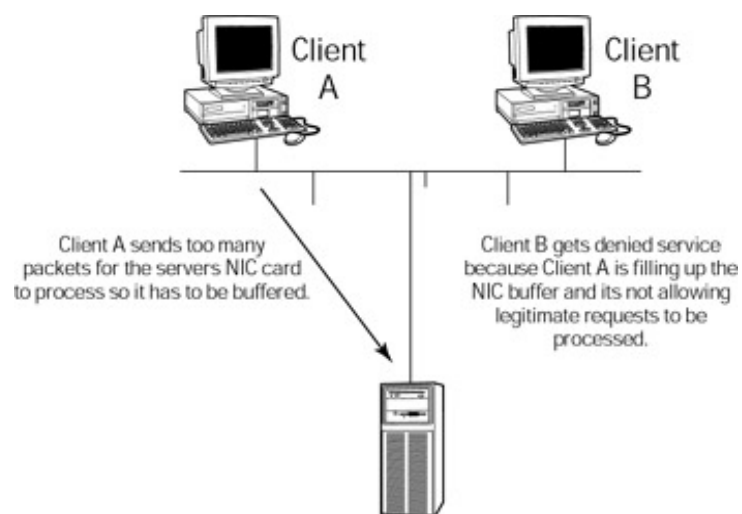


Figure 1-1: Typical Denial-of-Service Attack (Olsen, Loughran, 2002)

Operating System Threats

Security at the operating system level is what we are mainly interested in. There are two types of threats to the operating system, program and system. When one user writes a program and is used by another, misuse and unexpected behavior may ensue. Trojan horses and trap doors are some examples of program threats.

Program Threats

The Trojan horse (or just plain “Trojans”) is code disguised as some gentle program, which then behaves in an unexpected, and usually malicious way. The name comes from that fateful episode in the novel *The Iliad*, when the Trojans, during the battle of Troy, allowed a gift of a tall wooden horse into the city gates. In the middle of the night, Greek soldiers who were concealed in the belly of the wooden horse slipped out, unlocked the gates, and allowed the entire Greek army to enter and take the city. (Mirza Ahmad, 2002) The use of this program threat can easily be seen from the origin of the name.

Another program threat is the Trap Door. A trap door attack takes place when certain conditions occur. An example being the time of day in which certain commands are executed. Another example is what may occur when several commands are run at the same time. A common hacker

strategy is to install an application, then have it run only at a specified time.

The result of a trap-door attack is that the system is left vulnerable. (Stanger, Lane, Crothers, 2002)

System Threats

There are also system threats to the operating system. The two most common methods for achieving this misuse are worms and viruses. A virus is a destructive and malicious program designed to damage network equipment, including stand-alone computers. A virus has two parts: the part that starts and spreads the virus, and also the “payload,” (Stanger, Lane, Crothers, 2002) which is what the virus actually does to the operating system or file. Table 1-1 describes the types of viruses found in modern systems.

Virus type	Description
Boot sector/Master Boot Record (MBR)	This type of virus infects the first sector of a floppy disk or a hard drive. The boot sector is the part of a floppy that enables it to be read and written to. If infected with a virus, the floppy can then act as a transport mechanism for the virus. The MBR on most IBM-compatible systems is a similar place on the hard drive. Once a virus writes itself to the MBR, it can then generate activity that is either annoying (e.g., your system will play sounds at certain times of the day) or destructive (e.g., it will erase your hard drive).
File infecting	Some viruses attach themselves to legitimate programs. Launching the application activates the virus.
E-mail/Macro/Script	This type of virus is often found in e-mail attachments. Viruses such as Melissa and "I Love You" are all based on the VBScript computing language and exploit the trust relationships between Microsoft Office applications and the operating system. An end user must double-click on an e-mail attachment to activate the virus.

Table 1-1: Virus Types and Descriptions (Stanger, Lane, Crothers, 2002)

Some viruses will replicate or start-up simply when an application or hard drive is activated, or when an icon is double-clicked. A virus can also act as a “time bomb,” activating only after a certain number of days have gone by. Some time-bomb viruses activate only on certain days of the year, while others can conduct a logic attack, which means they will activate only under certain conditions. For example, a virus may replicate itself or deliver its payload only if a certain application is running on a certain day. Later, we will see how Windows NT handles and is protected from viruses.

The other major system threat is a worm. A worm is like a virus, except that a worm can spread from system to system without user intervention. The Nimda worm, which was released on September 18, 2001, was a particularly powerful worm that infected all unpatched IIS servers. It also spread to any Windows-based share. As a result, this worm had the ability to spread itself throughout a company LAN in seconds. This worm was able to spread so quickly because once it compromised a Web server, it then used that server to spread itself. As a result of this attack, Gartner Group, a respected consulting company, encouraged its customers to abandon Microsoft’s IIS in favor of other web servers while Microsoft worked to shore up IIS’s security against the Nimda worm. (Stanger, Lane, Crothers, 2002).

Windows NT Security

Overview

Even though Windows NT, or NT as it will be referred to as from now on, was originally meant to replace Windows, it has evolved into a platform for reliable network servers. Microsoft currently sells two versions of NT:

- *Windows NT Workstation*: Used as a general client operating system but more expensive and stable than Windows 98.
- *Windows NT Server*: Used as a server operating system.

(Strebe, Perkins, Moncur, 1999)

There are many similarities between the two versions. As a matter of fact, the main difference is in what the software license allows you to do and also the price of the product. Windows NT Server is usually the platform of choice for servers, so users expect more from it in when dealing with security.

Even though NT was originally designed with security in mind, it wasn't used widely for networking at first, and consisted of many security problems. Microsoft has improved its security significantly, but there are still security holes.

In order to keep your network secure, you need to know how your network operating system implements security. Similar to if you want to

keep a building secure you need to know what kind of locks are where, who has keys to those locks that use the building, and what other security mechanisms (motion detectors, timed or electronic locks, etc...) are in place within the building.

User Accounts

User accounts is where security all starts in a NT network. Starting from the logon prompt, you must supply a user name and a password. The purpose of the logon prompt is to allow the computer to identify the user and give them access to things he/she should (such as the files in your home directory) or should not be able to access (such as the files in the home directory of your boss). The logon prompt serves as the gatekeeper to your NT computer (see Figure 2-1).



Figure 2-1: The logon prompt identifies you to the computer and protects your network from unauthorized access (Strebe, Perkins, Moncur, 1999)

Each individual user should have an account even when there are groups of users that use the system for the same purpose. For example: an

office of data entry clerks should have their own account so when one user violates a security breach, the violation can be traced back to that user instead of the whole group of clerks who use the same account.

User accounts and group accounts that are only valid for a single NT computer are called *local user and group accounts*. On the other hand, there are user accounts and group accounts that are valid for all of the NT computers within a NT domain called *global or domain user and group accounts*. The local accounts are maintained by the computer on which they are valid. Each NT computer has it's own list of local user and group accounts, with the following exceptions: Backup Domain Controllers (BDC's) don't maintain any local accounts, and Primary Domain Controllers (PDC's) local accounts are the same as the network global accounts.

To clarify things, some of this terminology is summed up here:

Terminology

- *Local account:* A user or group account that only exists on the local Windows NT computer.
- *User account:* A security record maintained by Windows NT that records your user name, password, logon permissions, home directory, and other information pertaining to your individual use of the computer and the network.
- *Group account:* A record, maintained by Windows NT, of user accounts that are assigned access permissions as a group.

- *Global account:* A user or group account that is defined on the Windows NT Server Primary Domain Controller and may be used from all computers that are participating in the Windows NT domain.

(Strebe, Perkins, Moncur, 1999)

Using the Primary Domain Controller (PDC) and the Backup Domain Controller (BDC), the NT computer doesn't need to go any further than its own data structures to fix or resolve any security questions concerning local users and groups.

Security Subsystem

User mode and Kernel mode are layer components that perform many of the internal system operations in Windows NT. In order to have a better understanding of the NT security subsystem, here's a brief list of the components and their functions:

- *Log-on processes* – These are the user mode processes that are used to authenticate users when they log on to the computer system.
- *Local Security Authority (LSA)* – This component is used in conjunction with the log-on process to verify that an individual has a legitimate user account on the system. The LSA is the main component in the user mode portion of the security subsystem. The LSA is responsible for all interactive log-on activities and is the component that generates system access tokens (SATs).

- *Security Account Manager (SAM)* – Is currently called the *directory services database*, this User mode component is responsible for maintaining the user accounts database that is used by the LSA to validate an individual's account during the log-on process.
- *Security Reference Monitor* – The security reference monitor controls the internal security of the system by taking care of all access, creation, and deletion of objects within the system. It does this using the access control listing or ACL that is associated with each object. Each of these objects contains elements called *Access Control Entries (ACE)*. Each of these ACEs contains the unique security ID of a user or a particular group. The SID is actually a unique number generated by the operating system that describes each user or group within the NT domain.

(Hadfield, Hatter, Bixler, 1997)

For a better understanding of how a process accesses an object and the use of the Security Reference Monitor, see Figure 2-2.

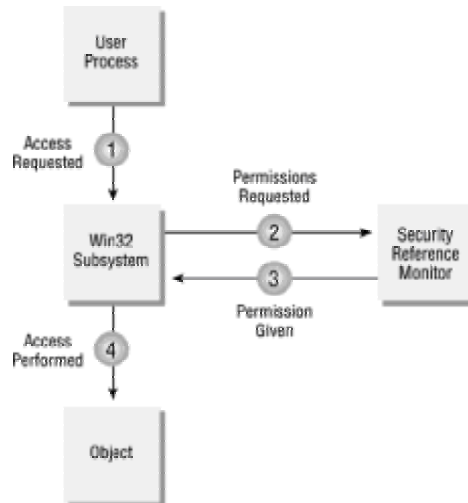


Figure 2-2: The Win32 subsystem performs object accesses for processes, and the Security Reference Monitor informs the Win32 subsystem whether an access may be performed. (Strebe, Perkins, Moncur, 1997)

In Windows NT, when a user is created by the system administrator, that user account is assigned a unique security identification number (SID) by the operating system. The SID represents the user account just as long as it's active on the system. If the user gets deleted from the system and later re-added to the system, a completely new security ID will be assigned to the individual's account. This new security ID won't retain any of the old security attributes from the user's previous account.

Objects and Permissions

Users have access tokens that identify them and the groups they belong to. In order for Windows NT to enforce security for these users, there need to be some rules about which resources each user may access in the

computer. That's what this section is about---objects (the resources) and permissions (the rules).

In the physical world, keys unlock things that you want to protect, such as a filing cabinet containing confidential papers. In the computer world, SIDs are the keys. In a computer you want to protect files, directories, printers, and other resources that might be altered, destroyed, consumed unfairly or inappropriately, or that might contain information that you don't want made public. The locks that protect these resources in the Windows NT operating system are called *objects*, and they prevent access, just like the lock on a filing cabinet.

These objects are much more sophisticated than the physical locks that you may be used to, however. As you'll see shortly, Windows NT associates an object with just about anything you can think of, but file and directory objects are the objects that network administrators are most concerned with. Objects in Windows NT include (but are not limited to): directories, ports, symbolic links, devices, printers, windows, processes, files, network shares and threads. (Strebe, Perkins, Moncur, 1999)

*Note: Processes, which contain access tokens and manipulate objects, are also themselves objects. This is because processes can manipulate other processes by starting them, stopping them, increasing or decreasing their priority, and so on. Processes belonging to one user must be protected from other users' processes, so processes are objects too.

Services: What Objects Do

There are many things a process can do to a file if it has *permission*. It can read the file, write to it, or delete it. The things a process can do with an object are called the object's *services*. For example, a file's services include: open, close, delete, change, read, take ownership, write, change permissions. The object also contains other information about itself, including its name (the file name in the case of a file object), the object data (the contents of the file if it is a file), and an access control list that describes the users and groups that may use the object's services. Figure 2-3 illustrates a file object's type, services (permissions), and attributes.

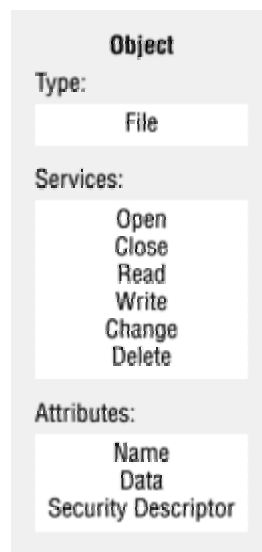


Figure 2-3: A file object has a type, services, and attributes. (Strebe, Perkins, Moncur, 2002)

Virus Protection

Windows NT is immune to executable file viruses just as long as you're not logged in as the administrator when installing software. But, NT cannot prevent the spread of viruses that come from files like office documents that most people have write access to because of the non-executable form.

In order for a virus to take effect to a certain program, the user loading that program must have write access to the executable file doing the loading. "As soon as you hit an actual system file, Windows NT will pop up with an Access Denied message, usually aborting the executable load." (Strebe, Perkins, Moncur, 1999). Usually you don't know what's happening and you'll probably blame NT but virus propagation is stopped cold by Windows NT security.

But, users who run files on their Windows 98 computers that store them on a NT server don't have such protection. "Just because a virus can't spread to a NT server doesn't mean a NT server can't spread it." (Strebe, Perkins, Moncur, 1999) Client operating systems see NT as just a big shared hard disk, so any executable files they copy to a NT server containing viruses will still contain viruses. You won't be able to load them on the server itself, but other users will be able to load them on other client

computers running Windows 98 or earlier. This is somewhat analogous to a carrier organism that is itself immune to the effects of a virus but that is still contagious to other organisms.

Conclusion

At this point, one should now have a better understanding of Windows NT security and some of the concepts that are associated with it. The fact that NT has such a strong user and group organization, has a very strong defense against viruses, worms and Trojan horses, and associates an object with almost anything you can think of, makes Windows NT the operating system of choice among many companies. The aspects of Windows NT that have been covered are user accounts, the security subsystem, objects and permissions, and Windows NT's inherent security. Also, a brief description of security itself has also been discussed.

Bibliography

World Wide Web

Books24x7 Database

- 1). Olsen, Keith; Loughran, Don, CIW Foundations Certification Bible. Hungry Minds publishing, 2002.
- 2). Mirza Ahmad, David R., Hack Proofing Your Network. Syngress, 2002.
- 3). Stanger, James; Lane, Patrick T.; Crothers, Tim, CIW: Professional Study Guide. Sybex, 2002.
- 4). Strebe, Mathew; Perkins, Charles; Moncur, Michael G., NT 4 Network Security. Sybex, 1999.
- 5). Hadfield, Lee; Hatter, Dave; Bixler, Dave, Windows NT Server 4 Security Handbook. Que, 1997.
- 6). SecurityStats.com, Virus Related Statistics; ©SecurityStats.com, Inc 2000, <http://www.securitystats.com/virusstats.asp>