



SecureNT White Paper

Corporate contact:

Marco Peretti
mperetti@securewave.com

DigitalWave S.A.	Tel: +352.315126
18, Rue Jean Marx	Fax: +352.315127
L-8250, Mamer	
Luxembourg	www.securewave.com

Copyright © 1998-1999 DigitalWave S.A.
All Rights Reserved

Introduction

This paper describes in detail SecureNT version 1.2. SecureNT is a security toolkit that allows you to lock and unlock I/O devices such as the floppy drive, the CD-ROM, LPT, and COM ports of a Windows 95/98/NT workstation. As mentioned in the Windows NT resource Kit, no operating system can provide physical security for your computers because external media drives (floppy disk, CD-ROM, etc.) provide the physical means for anyone to bypass Windows and gain access to your files. You should be aware that the American Society for Industrial Security estimates that 77% of security breaches come from the inside and hence it is imperative to control who has access to external media drives. SecureNT is the only tool on the market that allows you solve once and for all physical security problems.

SecureNT can not only be used to secure your company's LAN but also to prevent end-users to modify the software configuration of their workstations by installing unauthorized applications and therefore simplifying maintenance of large networks.

It is a well-known fact that most viruses come from end-users' floppies and that often these floppies circulate from PC to PC. By preventing users from using floppies altogether you will be able to reduce considerably the risk of introducing new viruses. SecureNT can do much more than just lock the floppy drives. SecureNT can lock/unlock all I/O devices and even grant/deny usage based on groups' membership.

Configuration

SecureNT consists of a client portion, to be installed on all workstations, and a GUI application known as 'SecureNT Administrator'. The client portion is available either as a native Windows NT Service or as a native Windows 95/98 VxD. A Windows NT Service is an executable that is run in a protected context and is subject to Windows NT security mechanisms. Services are automatically started at boot time and end-users cannot stop/kill them under any circumstance. Only system administrators can start/stop services and as such they are the preferred solution to implement secure sub-systems under Windows NT¹. Under Windows 95/98 we had to hide and protect our VxD since system components cannot be protected as when running under Windows NT. Our VxD is capable of auto-loading itself. In other words, no entries in system.ini or in the registry are necessary. Just install the VxD and the PC will be protected. And there is more. The VxD can be given any name you wish and its timestamp is set to hide it within all system ones. And even if a smart user finds out the location of our VxD he/she will not be able to do much. Our auto-replication feature will prevent users from tampering (deleting, replacing, etc.) the file and, if necessary, it will create another instance of itself. Only authorized Administrators can disable the VxD.

¹ We recommend as well NTFS and change the PC BIOS settings to boot from the hard-disk only.

For better security under Windows 95/98 we do recommend to change the boot sequence from c,a to a,c to prevent the user booting in DOS. It is also very important to configure Windows so that the user is not allowed to boot in DOS by pressing either F5, F6 or F8 during the Windows Boot.

The Service and the VxD are functionally equivalent and from here onward we will refer to them as the SecureNT Service. The main difference you should be aware of is that the Windows 95/98 client v1.2 is only capable of locking floppy drives and CD-ROMs. Other devices will soon be added.

As soon as the SecureNT service is installed and started all Floppy Drives, CD-ROMs, COM & LPT ports are locked. SecureNT can handle multiple floppy drives (3.5", 5.25"), Iomega Zip Drives, and multiple CD-ROMs (IDE and SCSI). If a Serial Mouse is present on a COM port then the port will not be locked. Each device will be described in a later section.

Hence, in its simplest and most common configuration, you just have to install the SecureNT service². The service can be easily installed from a remote location using any software distribution package such as Microsoft SMS or even simple batch files.

With SecureNT you can implement sophisticated security policies either using the SecureNT Administrator application or by assigning users to special groups. Next section describes the SecureNT Administrator.

SecureNT Administrator

The SecureNT Administrator is a Windows NT GUI application (shown in figure 1) that allows authorized administrators verify, grant, and revoke access to any I/O device on any workstation on your LAN from their PCs. No need to walk around the company with a bunch of keys to operate hardware locks.

Only members of the 'SecureNT Admins'³ group can run the SecureNT Administrator application. This solution has a number of advantages. First, only authorized personnel can grant/revoke usage of an I/O device. Even if an end user manages to get hold of the application he/she will not be able to run it. Second, you do not have to assign system privileges to SecureNT administrators. For instance, this mechanism allows you to designate help desk personnel as SecureNT administrators without having to grant them system administrators privileges.

² Single executable, no DLLs, no external dependencies.

³ Global group to be created on your Primary Domain Controller

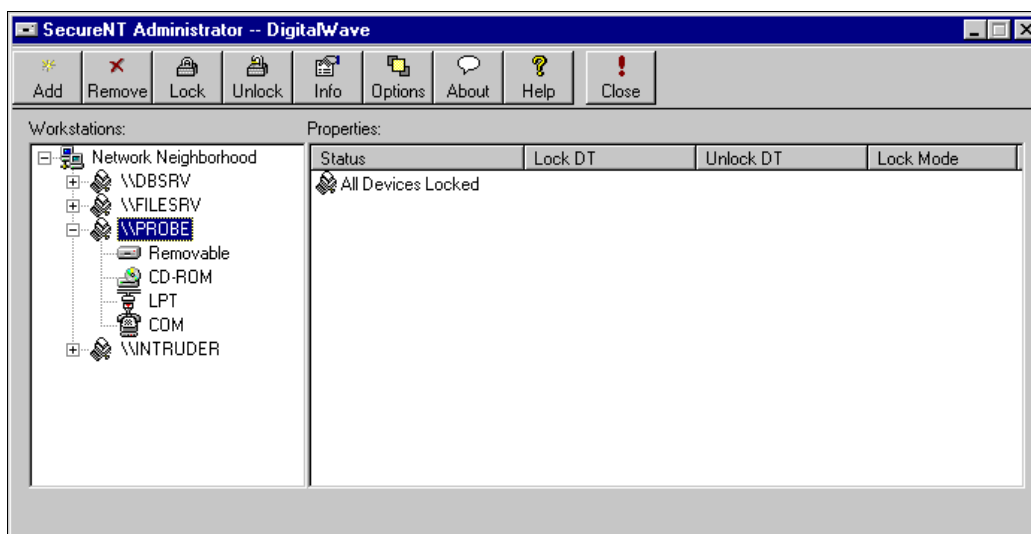


Figure 1: Main screen of the SecureNT Administrator application

The SecureNT Administrator application has been designed to minimize the workload of the administrator. The application thus contains only the workstations for which you are managing an I/O device -- all other workstations are assumed⁴ to be locked. This is a great time saver in networks with hundreds of workstations. Moreover, by keeping the workstations in the local network neighborhood to the minimum the administrator can concentrate on the workstations for which he/she is allowing access to an I/O device. As soon as the workstation is fully locked it disappears from the list.

SecureNT Administrator has been designed to manage what we consider *exceptions*. Let's have a look at a typical scenario to see how SecureNT Administrator is used in practice.

Example:

User A calls the SecureNT Administrator because he/she needs to use the CD-ROM. The administrator has to add the user's workstation on the local network neighborhood list. He/she can do so either by selecting the workstation's name from a list of workstations or select the user name from another list and then selecting the workstation (where he/she is logged on). We have implemented two mechanisms to select the workstation name because, in some companies, users have no easy mean to find, and hence tell the administrator, the name of their workstation. Given a user name we are able to detect where he/she is logged on and present a list⁵ of workstations to the SecureNT administrator.

⁴ If SecureNT Service has been installed then they are locked.

⁵ He/she could be logged on more than one workstation.

Once the workstation has been added to the local network neighborhood, the administrator can verify its status and grant/revoke usage on the chosen device.

For instance, to unlock the floppy, he/she would select the floppy and click on the 'Unlock' button. SecureNT allows the Administrator to unlock a device unconditionally⁶, or set a *time limit* after which the device will automatically re-lock itself. An example is shown in figure 2.

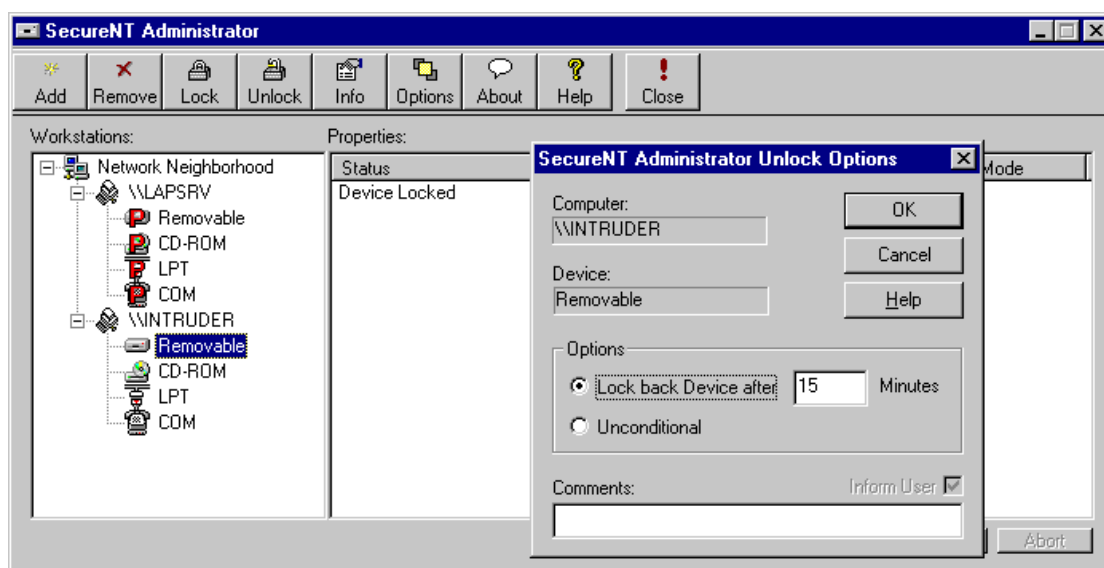
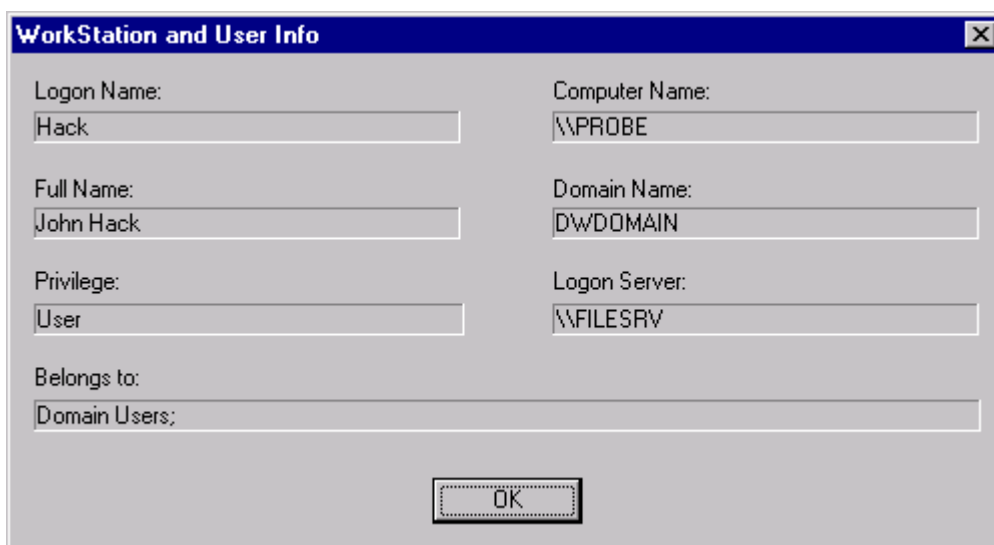


Figure 2: Unlocking the floppy drive on INTRUDER

Even in case of network failure, the Windows NT Service will lock-back the device after the number of minutes you have specified have elapsed. A log of all lock/unlock activities is stored, under Windows NT, in the event log. Moreover, under both Windows NT and Windows 95/98, devices are unlocked for the duration of the session only. As soon as he/she log off (or reboots, etc.) all devices are locked back.

SecureNT provides as well important information regarding logged on users. The SecureNT Administrator can verify the user identity and logon statistics by simply selecting a workstation (from the local network neighborhood) and clicking on the 'Info' button. An example of such statistics is shown in figure 3.

⁶ Until he/she logs off, reboots or the SecureNT Administrator re-locks it.



Logon Name:	Hack	Computer Name:	\\PROBE
Full Name:	John Hack	Domain Name:	DWDOMAIN
Privilege:	User	Logon Server:	\\FILESRV
Belongs to:	Domain Users;		

OK

Figure 3: User Information

It is very important to understand that SecureNT administrator is a tool to be used only to grant access to an I/O device for a *limited period of time*. If you wish to grant *permanent access* to an I/O device to one or more users then you should assign them to one of SecureNT groups.

SecureNT Groups

There are a number of groups that you can use to grant permanent access to one or more I/O devices plus two administrative groups. These groups have to be created by your system administrator on the primary domain controller exactly as shown below.

SNT_FLOPPY: grant use of floppy and other removable media such as Iomega Zip Drive.

SNT_CDROM: grant use of the CD-ROM(s)

SNT_COM: grant use of the parallel port(s)

SNT_LPT: grant use of the serial port(s)

SNT_ALL: grant use to all devices.

As with any other group, if you associate a user with a group while he/she is logged on he/she will have to log off and log on.

During the logon process, SecureNT will examine the access token of the user logging on and will automatically unlock I/O devices according to the groups that the user belongs to. The devices are automatically re-locked as soon as the user logs off.

It is therefore very important to protect *all* workstations in your LAN since, most of the times, users are allowed to log on any workstation.

There are well two additional groups that you can use to define who can use the SecureNT Administrator application.

SNT_ADMINS: grant use SecureNT Administrator Application. This simple yet powerful delegation mechanism allows you nominate SecureNT Administrators without having to grant system privileges.

SNT_HELPDESK: grant use of the SecureNT Administrator Application but the user is not able to change the status of any devices. Still useful to determine the cause of a user problem.

New in Version 1.2 is the support for **LOCAL GROUPS** under Windows NT. Local groups are not available under Windows 95/98. The Administrator is now able to configure LOCAL users by associating them to one or more of the SNT_ groups described above (except SNT_ADMINS and SNT_HELPDESK) to customize off-line or stand-alone computers. In practice, the Administrator has only to manage local users and local groups using USER MANAGER on the Workstation he/she wishes to configure.

Devices

SecureNT can already handle⁷ quite a few devices but we will certainly add more based on the feedback received. For instance, recent tests confirmed our ability to disable the keyboard, the mouse, and even more devices.

Below you will find a list of I/O devices currently managed by SecureNT.

Removable Media

SecureNT supports all types of floppy drives and even removable drives such as Iomega Zip drives. SecureNT inspects your workstation physical configuration and locks all drives it finds. Removable drives are assigned an ACL⁸ and administrators aren't affected. If a user tries to use the floppy drive while it is locked he/she will receive a message stating that access is denied as shown in figure 4.

NB: The messages cannot be customized because they are generated by the Windows security sub-system. Moreover, these messages will be shown in the language of the Windows version installed.

⁷ Devices are locked for both Windows and DOS applications.

⁸ Access Control List



Figure 4: Access Denied while trying to use the floppy

CD-ROM

SecureNT supports both IDE and SCSI CD-ROMs. It does not matter if CD-ROMs are internal or external. SecureNT can handle an unlimited number of CD-ROMs. CD-ROMs are assigned an ACL and administrators aren't affected. If a user tries to use the CD-ROM while it is locked he/she will receive an error message stating that access is denied (as for the floppy drive).

COM & LPT Port

COM and LPT ports are locked with a different mechanism. The service enumerates and opens all physical ports it finds. Since a port cannot be shared between processes the ports appears as locked. SecureNT is smart enough to detect and skip COM ports used by serial mouse drivers.

It is worth noting that local printers are NOT locked but all other applications using LPTs are. However, local printers can still be protected by System Administrators. It is sufficient to remove the 'Everyone' group from the list of users having access to the printer.

Conclusions

SecureNT provides the same level of security as hardware locks at a fraction of the price. I/O devices can be locked and unlocked from a remote workstation using the SecureNT Administrator application and users can freely move from a workstation to another because rights are associated to the user, not the workstation.