ADMINISTRATION TECHNIQUES FOR IMPLEMENTING SECURITY ON LARGE WINDOWS NT NETWORKS

Alessandro Augusto
Instituto de Computação
IC - UNICAMP
13083-970 Campinas - SP
alessandro.augusto@ic.unicamp.br

Célio Guimarães
Instituto de Computação
IC - UNICAMP
13083-970 Campinas - SP
celio@ic.unicamp.br

Paulo Lício de Geus
Instituto de Computação
IC - UNICAMP
13083-970 Campinas - SP
paulo@ic.unicamp.br

ABSTRACT

The process to secure a Windows NT computer can be easy if the administrator knows which configurations and security settings he needs to do. But, even when the administrators knows the changes that needs to be done on a single NT computer, the process to apply the same configuration in an environment with hundreds of NT-based computers can be really frustrating. Most solutions to this problem require some expensive tool such as Systems Management Server (SMS). But there are many companies and institutions that cannot purchase this kind of tool or the SMS's licenses. In this case, the solutions presented until now don't solve the problem of administering NT and applying security to a NT network. This paper describes some highly security recommendations and propose three solutions to solve the difficulty to apply security or to upgrade NT-based computer networks without any extra tool.

1 INTRODUCTION

During the last years it is unquestionable the advantages that institutions had with the increase in the use of computers, with the interconnection of these computers in networks and with the sharing of resources. Even so, it is also unquestionable that the institutions need to be prepared before migrating to this new "digital territory".

Thus, these have been discussion a lot on system administration and security, especially in UNIX operating systems, but little aspect deals with Windows NT operating system. Among the operating systems with wide prominence and use in several environments, Windows NT gets the attention with its growing use and its user-friendly interface.

In spite of easiness to use the system, comparing Windows NT with other UNIX systems, NT can be considered "lacking" in the subject of network administration, especially when the topic is applying security on a NT network.

In institutions that have a considerable group of interconnected computers through a network based on Windows NT, it always existed difficulties when the administrators need to do apply some security configurations on each network computer. These difficulties generate high monetary costs to maintain a group of system administrators in service.

Windows NT's environments has a reputation to be a system requiring hands-on administration, that is, it needs a manual by-hand work [4]. It is necessary the administrator's physical presence in each one of the machines every time it needs to do some modification or configuration. With that, it can be concluded that the associated costs would increase as the amount of the network computer gets bigger. Remote software installation and configuration is another problem in this kind of environment.

A large portion of configuring security on NT is modifying some Registry values. As the administrator begins to look at configuring values keys on the Registry and to read the papers about NT security, he starts to think that it is almost impossible to administer NT-based computer networks without some expensive administrative tool such as SMS (Systems Management Server) and without a large number of system administrators available [6]. For a practical example, the usual software installation methods on NT requires the administrator to sit in front of an individual machine, answer some questions interactively, wait some minutes for the software to load and maybe reboot the machine. This approach doesn't scale to hundreds of NT machines. With this example, the administrator can't imagine the problem that he will face when he starts to configure security. He knows what he needs to modify on the Registry, but how does he do all this modifications without sitting in front of each computer?

The goal of this work is to define a good level of security for NT computers and also, to create techniques and propose solutions, where the system administrator is able to configure the security and have it automatically distribute to each machine of a given type. But there are some restrictions about these techniques, one of the restrictions is that the administrators cannot copy the whole Registry and paste it on another computer.

Fortunately, there are ways to by-pass most of these problems. As a result, the solutions presented

here solve this problem of applying security on NT network and also, techniques to facility any software installation, software upgrading and also any other kind of communication between the workstations and the server without expensive tools such as SMS. For another example, if the administrator needs to know the exactly time that each network computer was turned on, he can create a batch script that logs the time and use this script with one of the proposed solutions to send these logs to the administrator.

The techniques presented in this paper can be considered good solution for institutions that don't want spend money with this kind of problem. With these techniques, system administrators can deploy up to 100 PC's per hour depending on which technique he chooses and also, it depends of the package size that is being installed. These techniques will increase a lot the deploy ratio and turn much more easily the administration process.

This paper is structured. After a brief introduction on section 1, it describes the Windows NT operating system on section 2. After that, it describes the Registry and the problem on how to administering the NT network, respectively on sections 3 and 4. Section 5 presents some security recommendations. Section 6 proposes and explains the solutions to administer the NT networks. Section 7 shows a practical example with its solution of how can the administrator applies some security configurations to a NT environment. The paper finishes it with the conclusion and the references used by it.

2 WINDOWS NT

Since its initial release in 1993, the operating system Windows NT[1] appeared as an outstanding operating system with multiple purposes. Projected to integrate a client-server network, Windows NT is divided in two products: Windows NT Workstation and Windows NT Server [7].

Combining an application server with a file system and a print system, it was created to be easy to use and to manage. Besides that, it is much more reliable and stable than the previous versions of the systems Windows 9.x and Windows 3.x.

The client is known as Windows NT Workstation. The default system already brings applications to execute in the network such as ftp clients, electronic mail, telnet, etc. In the same way, NT Server default system brings some different applications, for example a web server, IIS[2].

In Windows NT, all configurations are stored centrally in only one database denominated Registry, which is one of the most important topics about this system, especially when deals about security [5].

3 REGISTRY

Registry is a central and organized database that contains all the information about hardware and software configuration.

In previous versions of Windows, configuration files with extension .ini and .sys executed the functions exercised by the current Registry. The problem of these configuration files was the restriction with relationship to its maximum size to be of 64 Kb. Beyond that problem, any user could easily edit some configuration file and could cause damage on it [5].

Inside of the Registry is stored all information about user's account, user's groups, besides information about all hardware and software installed in the computer.

To modify the Registry values, it is necessary to have writing permission, because each of its items has access permission.

Every change in the Registry affects the configuration of the machine directly.

Developed with a hierarchical structure, the Registry can be compared with a country, which it is divided in states, which is divided in cities, in neighborhoods and so on.

4 THE PROBLEM

One of the hardest tasks that system administrators have with NT environment is to configure the security of its network and to install or upgrade software. Some people don't agree with this, they say it's much easier to install an application under Windows NT than under UNIX. On NT, the administrator just need to put the CD or the floppy in the drive, maybe click setup (if autorun is not configured automatically), answer some Installshield questions and wait for it goes to work [4]. These people would expect that UNIX software management would be much harder, since there is no installshield there.

The argument that NT is easier to administer due to its graphic interface (GUI-based) it is questionable. Besides being questionable due other operating systems also possess graphic interface, it is also doubtful the argument that the graphic interface is simpler than command line interface (CLI-based). Generally, GUI-based tools are easier to install but harder to automate and extend [4].

However, the fact that software installation under NT is easier than UNIX can be considered true for an isolated NT machine. Managing a large

[1] New Technology
[2] Internet Information Server

environment is entirely different. Command-line tools are easier for any system administrator to use when managing a large environment.

The difficulty found in Windows NT administration occurs when the environment, which is the amount of network computers, is larger than 1. The difficulty and the time spend in the administration is directly proportional to the amount of computers. The larger is the amount of computers in the environment, more complex and delayed will be its administration.

Another item that hinders the administration of Windows NT networks, is the fact of having a heterogeneous network, that is, when there are computers with different hardware profiles.

In spite of the same security configuration in two different machines add or modify the same keys and fields in the Registry, it is impossible to copy the Registry of the first computer and paste into another NT computer where it was not configured yet. The impossibility is because of the remaining keys, which contains hardware and software configurations specific to each computer.

The two main problems here are: (1) what changes and security settings should the administrator do to make a NT computer secure? (2) How to apply these settings to the whole NT network computers without having to sit in front of each machine? How to administer a Windows NT network and its security in some easy way, also with a cheap solution and fast results, considering the amount of computers present in the network is larger than 1? How to do the needed modifications in all the network machines with a small effort and in the least possible time? How to automate the tasks of software installation or upgrading to the remaining network machines? The solutions for these questions are describe in the next sections.

5 SECURITY SETTINGS RECOMMENDED

Windows NT provides a rich set of security features, however, the default configuration is highly relaxed. This is because the operating system is sold as a shrink-wrapped product with an assumption that an average customer may not want to worry about a highly restrained but secure system on their desktop. This assumption has changed over the years as Windows NT gains popularity largely because of its security features [10].

This section describes the most important security recommendation settings. It will follow some recommendations of a Windows NT C2 configuration [11].

A particular installation's requirements can differ significantly from another. Therefore, it is necessary to evaluate the environment and requirements before implementing a security configuration.

Windows NT allows the administrator to establish a full range of security levels, from no security at all to the C2 level of security. These levels are arbitrary, and the administrator will probably want to create his own level by blending characteristics of the levels presented in this section.

One reason to not have maximum security level at all times is that the limits the administrator sets on access to computer resources make it a little harder for people to work with the protected resources. And if the security is too tight, users will try to circumvent security in order to get work done [10].

The first step in establishing security is to make an accurate assessment of the needs. Then choose the elements of security that the administrator wants, and implement them.

The following subsections describe some recommendations to apply security configuration on Windows NT.

5.1 Operating System and Service Pack Installation

The first step to start armoring the NT system is the operating system (OS) installation. Install it on a NTFS file system. With NTFS, the administrator can assign a variety of protections to files and directories, specifying which groups or individual accounts can access these resources in which ways. During the OS installation, select only the services that will run and the protocols that will be need. The fewer services that are running, the fewer exploits or security issues the system will have [10].

Following the installation, install the latest service pack (current service pack 6a). Staying current with the latest exploits is critical for a secure system.

Once the administrator finishes the OS and the service pack installation, he can start to configure the system. All unnecessary devices and services must be disable. The services that should be enable depend of the needs.

5.2 OS/2 and Posix Subsystems

OS/2 and Posix are subsystems designed to run with other system but not specifically with Windows NT and that may not be able to take full advantage of all Windows NT features (such as memory management).

Most of the administrators don't need these subsystems, so it can be disable. To remove OS/2 and POSIX subsystems, the administrator needs to

delete the \winnt\system32\os2 directory and make the following Registry configurations [11]:

Table 1- removing Posix and OS/2 subsystems.

Hive	**HKEY_LOCAL_MACHINE\ SOFTWARE**
Key	\Microsoft\OS/2 Subsystem for NT
Action	Delete all sub keys
Hive	**HKEY_LOCAL_MACHINE\ SYSTEM**
Key	\CurrentControlSet\Control\Session Manager\Environment
Value Name	Os2LibPath
Action	Delete
Hive	**HKEY_LOCAL_MACHINE\ SYSTEM**
Key	\CurrentControlSet\Control\Session Manager\SubSystems
Value Name	Optional
Action	Delete values
Hive	**HKEY_LOCAL_MACHINE\ SYSTEM**
Key	\CurrentControlSet\Control\Session Manager\SubSystems
Action	Delete entries for Posix and OS/2

5.3 ShutDown Button

Normally, any user can shut down a computer running NT without logging on by choosing Shutdown in the Logon dialog box. This is appropriate where users can access the computer's operational switches; otherwise, they might tend to turn off the computer's power or reset it without properly shutting down. However, the administrator can remove this feature requiring users to log on before shutting down the computer [10]. The configuration to remove the shutdown button from logon dialog box is on table 2.

Table 2- remove shutdown button from dialog box.

Hive	**HKEY_LOCAL_MACHINE\ SOFTWARE**
Key	\Microsoft\Windows NT\ CurrentVersion\Winlogon
Value Name	ShutdownWithoutLogon
Action	Set the value 0

5.4 Files and Directories

Among the files and directories to be protected are those that make up the operating system software itself. The standard set of permissions on file system and directories provide a reasonable degree of security without interfering with the computer's usability. For a high-level security installations, however, the administrator might want to additionally set directory permissions to all subdirectories and existing files. To protect the files and directories, the administrator needs to use the ACL editor in Windows NT Explorer to change access on the system drive (by default "C:\") to grant full control to Administrators and SYSTEM, and grant read permission to Everyone. In [10] and [11] it gives the following recommendations:

Table 3 - protecting files and directories.

Directory	**Permissions**
C:\	Administrators: Full Control SYSTEM: Full Control Everyone: Read
\WINNT	Administrators: Full Control SYSTEM: Full Control Everyone: Read CREATOR OWNER: Full Control
\WINNT\ REPAIR	Permit only Administrators: Full Control
\TEMP	CREATOR OWNER: Full Control
\WINNT\ Profiles\ <user>	User: Full Control
\WINNT\ Profiles\ administrator	Remove Everyone

5.5 Protecting the Registry

In addition to the considerations for standard security, the administrator of a high-security installation might want to set protections on certain keys in the registry. By default, protections are set on the various components of the registry that allow work to be done while providing standard-level security.

For high-level security, the administrator can assign rights to specific registry keys, but this should be done with caution, because programs that the users require to do their jobs often need to access certain keys on the users' behalf.

Normally, the keys in the registry are changed indirectly, through the administrative tools such as the control panel. The registry can also be altered directly with any registry editor.

Open regedt32.exe and grant full control to Administrators and SYSTEM and read access to Everyone for the followings Registry subkeys [11]:

- HKEY_LOCAL_MACHINE\Software : locks the system in terms of who can install software.
- HKEY_LOCAL_MACHINE\Hardware
- HKEY_LOCAL_MACHINE\System

- HKEY_USERS\.Default

5.6 Restricting Remote Access to the Registry

The default permissions do not restrict which users can have remote access to the registry. Only administrators should have remote access to the registry.

To restrict network access to it, select the hive HKEY_LOCAL_MACHINE\System, the key CurrentControlSet\Control\SecurePipeServers and the value name winreg and set the Administrators permission to full control, and make sure no other users or groups are listed [1]. Table 4 shows this configuration.

Table 4 - restricting remote access to the registry.

Hive	**HKEY_LOCAL_MACHINE\ SYSTEM**
Key	\CurrentControlSet\Control\ SecurePipeServer
Value Name	Winreg
Action	Administrators: Full Control

5.7 Trojan Horses

Restrict untrusted users' ability to plant Trojan horse programs on the system. Trojan horses can take advantage of the Run utility if its is unguarded [14]. There are some trojan horses that are written to execute during an Uninstall operation.

To restrict the ability of users to plant trojan horses programs, set the values of table 5.

Table 5 - protecting from trojan horses.

Hive	**HKEY_LOCAL_MACHINE\ SOFTWARE**
Key	\Microsoft\Windows\CurrentVersion
Value Name	Run, RunOnce, Uninstall, AEDebug
Action	Everyone and all untrusted users: Read

5.8 Share

To allow only the administrator to control which users can access a computer from its network interface and what information is shared over the network interface set read permission for Everyone and all untrusted users on the value of table 6 [11].

Table 6- shares.

Hive	**HKEY_LOCAL_MACHINE\ SYSTEM**
Key	\CurrentControlSet\Services\ LanmanServer
Value Name	Share
Action	Everyone and all untrusted users: Read

5.9 Cache Logon

The default configuration of Windows NT caches the last logon credentials for a user who logged on interactively to a system [1]. Even though the credential cache is well protected, administrators may want to disable the cache. This results in a somewhat longer logon time, but prevents malicious users from tapping logon information from short-term memory. Table 7 shows how to disable caching.

Table 7 - disabling cache logon.

Hive	**HKEY_LOCAL_MACHINE\ SOFTWARE**
Key	\Microsoft\Windows NT\ CurrentVersion\Winlogon
Value Name	CachedLogonCount
Action	Set the value 0

5.10 Hiding the Last User Name

By default, Windows NT places the user name of the last user to log on the computer in the user name text box of the logon dialog box. This makes it more convenient for the most frequent user to log on. To help keep user names secret, the administrator can prevent Windows NT from displaying the user name from the last log on [13]. To prevent it, the administrator needs to set the values of table 8.

Table 8 - hiding the last user name.

Hive	**HKEY_LOCAL_MACHINE\ SOFTWARE**
Key	\Microsoft\Windows NT\ CurrentVersion\Winlogon
Value Name	DontDisplayLastUserName
Action	Set the value 1

5.11 Fpnwclnt.dll

There is a security issue that may occur due to the way Windows NT handles the file \winnt\system32\fpnwclnt.dll. This file is a dynamic link library that let files and prints services for a netware and directory service manager for netware perform password synchronization with Novell netware servers. If there is no Novell netware servers on the NT network, this file should be removed [12].

5.12 User Rights and More Security Configurations

Above, the paper described a few recommendations to set a Windows NT as a C2 security level. There is a lot more security configurations that can be changed. There are several user rights that the administrators should be aware of and possibly audit. This permissions can be simple changed using the Microsoft Manager Console.

MMC integrates all the set of administration components. Together, these services provide a model of system administration and coherent delegation that reduces the time of administration. MMC hosts the programs, called snap-ins, that administrators use to manage their servers.

MMC allows administrators to configure account police, local polices, event log, restricted groups, system services, registry and file system.

The security template snap-in is a stand-alone Microsoft Management Console (MMC) snap-in that allows the creation of a text-based template file that contains security settings for all security areas.

6 PROPOSED ADMINISTRATIVES SOLUTIONS

The first of the main problem present before is accomplished, which was the changes and security settings that the administrator should do to have a NT computer more secure then the default installation. Now the problem is how can the administrator applies these settings to the whole NT network computers without having to sit in front of each machine and configuring one by one?

To solve this problem, this paper proposes 3 techniques that will help the administrator. In order to decide on which technique would be easier to use, the system administrator needs to evaluate and consider as many options as possible.

The procedure for any of these techniques has basically two steps:

1. create a package that will be installed or applied
2. choose the technique to apply the package created

For a better understanding, the term "change" is standardized in this paper as being the task or the modification that the administrator wants to do in his network computers. This change can be for example a simple modification in the standard wallpaper, or a new software installation, or to restrict the permission to read the Registry or any other alteration.

Also the term "model machine" defines the computer where the change was accomplished for the first time. This model machine can be any of the present computers in the network and it will be consider a reference during the whole process. The package will be created in this model machine.

"Target system" or "target machine" are the terms used to define the network computers where the changes accomplished in the model machine will be applied, that means, the computers where the package created will be installed.

Next section will detail the process to create the package.

6.1 Packaging

The heart of successful automated installations is the first step, which is called packaging. As the name says, packaging is the process to create a file, which contains all the changes that the administrator wants to apply in the network [3].

The packaging process is similar to the clone process.

With the impossibility of copying the whole model machine Registry to the target machines, the goal of the packaging is to create a system exactly equal, that is, to clone the model machine, including in the clone system all the configurations and security policy of the model machine, all them installed software and configured, besides considering each system as being a different machine in the network.

The initial idea of the clone process is to discover what changed in the NT system of the model machine after any change and to create a package just contends the modifications that happened after the administrator execute its change, it will be detailed better in the section 6.1.3. After creating the package, it needs to be applied in the target machines with some of the techniques that will be explained below.

When someone change any property in NT or when someone install a new software or hardware, new files and new keys are added and modified in the Registry of that system. The clone process seeks to discover which were those modifications. After discovering the modifications that were done in the model machine, it creates the package that will be applied in the target machines.

To discover the alterations happened in the model machine, it is necessary some application that does a "sweeping" of the file system and the Registry, to discover what changed in the system after the administrator's modification, and as result, create the package. In this paper the application used to sweep the system and to generate the package is called sysdiff.exe.

6.1.1 Sysdiff.exe

Sysdiff.exe[3] is a practical example of a tool that helps to clone NT systems. With this tool it is possible to discover all the new files that were added or modified in the file system and all the keys and values that were inserted or modified in the Registry.

The application Sysdiff.exe doesn't install the operating system, it just discovers the modifications happened in the model machine, it generates a package contends those changes and it creates an installation for that package.

To run correctly, there are some requires that need to be done for sysdiff.exe:

- It is necessary to define a "model machine", which is a reference computer, where the changes will be accomplished firstly. This model machine should run the same operating system of the target machines, where the package will be applied.

- It is also necessary to define a distribution point. A shared folder (share), where should be stored the application Sysdiff.exe and the package created. It is necessary that the target machines have access to this share.

The clone process should be fast enough, otherwise it can be unviable. Depending on the small number of network computers, the clone process can delay more than the accomplishment of the same task in all the target machines.

6.1.2 Options of the application Sysdiff.exe

Sysdiff.exe possesses the following parameters:

Table 9 - Options of sysdiff.exe.

Option	Command Line
/Snap	Sysdiff /snap snapshot_file
With this option, the application takes a snapshot of the current system configuration. The parameter snapshot_file is already the name of the file in which the photo of the current configurations will be recorded.	
Option	**Command Line**
/Diff	Sysdiff /diff snapshot_file package
This option generates the distribution package. That package is a file contends the differences found among the first snapshot token of the system, with the configuration of the system registered immediately after the changes are accomplished. The new parameter included in this option is the name of the package that will be create. This is the same package that will be applied in the target machines.	
Option	**Command Line**
/Apply	Sysdiff /apply package
This option is used to apply the package generated by the option /diff in the target system, that means, in the machine that is executing the application Sysdiff.exe.	
Option	**Command Line**
/Dump	Sysdiff /dump package dump_file
This option allows to create a report contends the modifications accomplished by a certain package. The parameter dump_file is the name of the file that will contains the changes applied by the package.	

6.1.3 Creating the package - step by step

After defining the necessary requires for Sysdiff.exe, described in the section 6.1.1, the steps to create the package are:

1. in the model machine, install the application Sysdiff.exe.

2. execute the application Sysdiff.exe with the option /snap to take a snapshot of the model machine before any change. This photo will contain all the configuration of the current NT system. This step should be done before the administrator configure any security setting.

3. Soon after, the administrator should accomplish the change wanted in the machine, e.g. accomplishes the security recommendations presented on section 5.

4. After accomplishing the configurations, execute the application Sysdiff.exe again with the option /diff. The objective of this step is to find the differences happened in the model machine and to create an installation package for the target machines. To create the package, Sysdiff.exe receives as entrance the snapshot took before the changes (step 2) and it supplies as result the generated package, which contains all the changes that were done on that machine by the administrator.

5. The last step is to leave the application Sysdiff.exe and the generated package in the share distribution folder (share).

With that, the process of creating the package is concluded. This stage is necessary to use with any of the techniques that this paper presents. Section 6.2 presents the first one, which uses a login account. The other one, uses NT Services and will be present in section 6.3. And the last technique, presented in section 6.4 uses the schedule service.

6.2 Solution 1: Using a special account

This technique is considered the easiest for networks where the physical location of each computer is close to the others.

The goal of this technique is simple: it discovers the entrances that were added in the

[3] Sysdiff.exe is a Microsoft tool, distributed on the Resource Kit CD-ROM. It can also be downloaded from the Web.

Registry of the model machine, creates a package and apply it on the target machines using a batch script.

To discover the modifications done in the model machine, it uses the process described in the section 6.1.3 to create the package.

This technique consists of:

1. Create an installation package for the changes that the administrator wants to do and leave it on a share drive (section 6.1.3).

2. Create a batch script (.bat), that connects the current machine to the above share and apply that package to this computer, the computer that is executing the batch (described on table 10).

3. Create a new user account login with administrator's rights and configure this account to execute the script from the last step (step 2) when the system administrator logon in.

4. On each target machine, the administrator should logon in using the user account create on step 3.

The goal of the batch script (from step 2) is to apply the package on every network machine. Suppose that the administrator already created the package, leave it on a share drive and created the new user account login. After this, the administrator needs to go to each computer, and logon in this new account. Then, the account will execute the script, which will do:

(1) connect the current computer to the share drive

(2) execute the sysdiff.exe application with the option to apply the package (sysdiff /apply)

(3) logout the account

With these steps, any modification on the first machine will create a new package. So the process to install or customize anything on the network can be really easy. The system administrator just needs to go to each network computer and logon in this new account.

6.3 Solution 2: NT services

This technique uses the concept of NT services. It came up for the system administrator that cannot be present on each network computer every time he needs to install a new package or do any other modification.

It is a good solution for companies and institutions that have a large environment, where the network computers stay far away from each other.

The solution is similar to the first one, but in this technique, the system administrator will need to go to each computer only one time, to configure the service, and not all the time that he wants to apply a new package.

Installing a new service, NT is capable to self-upgrade when the machine is booted, without any user interaction. The only requirement in this technique is to turn on the machine, so the system starts the service automatically and upgrades itself [10].

Among the benefits offered with the installation of the new service, there are:

- Possibility to automate tasks without needing administrator's interaction

- When applications are executed as being services, the applications are not concluded in the moment that an user makes the logout of the machine. The service will execute even if the user logout the system.

- If the application that is executed as service is a client-server application, this application can respond commands all the time, even when there is no user logged in the machine.

The second solution proposed by this paper consists of the following steps:

1. Create an installation package for these changes and leave it on a share drive (section 6.1.3).

2. Create a new batch file (.bat) different from the first technique. The batch file here should connect the current machine to the share drive where the package is, and compare if it needs to apply that package or not. Maybe that package has already been applied to the current computer.

3. Create a new NT service on each network computer and configure the service to be the batch file from step 2 and to startup automatically when the computer turns on [9].

In this technique, the administrator needs to create a batch file which will compare the packages from the share with the packages already applied on the current computer that is running the service.

With these steps, the system administrator needs to configure each computer only the first time, when he creates the new service. This service will run automatically when the computer turns on. So, every morning, when any user starts his work, he turns the computer on, and doesn't even know that the system is automatically self-upgrading.

6.4 Solution 3: Schedule Service

The third technique described in this paper is very similar to the second solution. It was deployed for the system administrator that can't be present on each computer during the upgrading.

This solution requires that the system administrator goes to each network computer one time and configure the NT´s schedule service to startup automatically. With this configuration, this service will always be startup when the computer turns on.

The schedule service allows the system administrator to schedule, remotely or locally, any task at some specific time. Also known as the AT

command, the schedule service is used to schedule tasks to run automatically at a present time.

The third proposed solution consists of:

1. Configure each network computer to start the schedule service automatically. This step is done just one time. The next times that the administrator applies different packages, this step can be ignored.

2. Create an installation package for the changes and leave the package on a share drive (section 6.1.3).

3. Create a batch file similar to the first technique (special account) which will connect the current computer to the share drive and apply the package on the current computer (table 10 shows the script).

4. Schedule the batch file created above to run at a specific time. There are options to schedule it to run several times, every day, every week, so it can be handled by the system administrator choices.

In [4], the authors say they were unsure with the schedule service because of security aspects. With the right configuration, schedule service is secure because only the administrator can schedule tasks to execute.

7 PRACTICAL EXAMPLE

For a practical example, suppose a NT-based network, with one server and 10 workstations. Also, suppose that the workstations are located at the same room and the server is in a different place, where the users don't have physical access.

The administrator wants to configure the security of each workstation and also wants to install a new software.

The steps to automate this tasks are:

1. The administrator selects one of the workstations and installs the sysdiff.exe application.

2. Before he makes any change, he executes sysdiff.exe with the option /snap to take the first snapshot of the machine.

3. After take the snapshot, the administrator starts to configure the security and the installation of the software. The paper won't get in details about what security setting the administrators is changing, but he can follow the recommendations described on section 5 of this paper and apply it here. The administrator installs the software in this step too.

4. When its done, the administrator executes the sysdiff.exe with the option /diff to create the package.

5. Now he needs to create a share drive (folder) and put the package created and the sysdiff.exe there.

6. The administrator needs to choose one of the techniques. In this case, lets suppose that the administrator choused the first technique described in this paper, the special account technique (section 6.2). The reason is because this solution is easier for network where the computers are close to each other's.

7. The next step is to create the batch script that connects the current computer to the share drive, and execute the sysdiff.exe with the option /apply (table 10).

8. After that, the administrator needs to create a new user account, with administrator's rights that will execute the script create on the last step.

9. To finish the process and to apply the package, the administrator needs to go to each workstation and logon in the special account that he created on step 8.

An example of a batch script is presented on table 10.

Table 10 - Batch Script.

```
@REM Script to automate and install security
@REM packages

@REM Packages are created with the application
@REM sysdiff.exe

@echo Applying the Package

@REM connect the current computer to the share
@net use g: \\share\drive

@REM Change the work directory
@g:

@REM Apply the package
@sysdiff /apply package

@REM Return to drive C:
@c:

@REM Disconnect from the share drive
@net use g: /d

@echo off
```

8 CONCLUSIONS

Automating NT tasks without administrative tools such as SMS can be by-passed using some techniques. The difficulty found to deploy this solutions was that all the published papers before this one, explain how it could be done assuming that SMS was installed.

After learning about NT application issues, Registry, and trying out various options, the paper suggest some security settings and proposes 3 solutions to apply this settings on every kind of NT-based environment, either when the amount of computers is small and the computers are close to each other, or in large environments and large networks where there is one system administrator that can't be in front of each network computer.

9 REFERENCES

[1] CERT. *Windows NT Configuration Guidelines.* April, 2000. Url: www.cert.org/tech_tips/

[2] EVARD, Rémy & LESLIE, Robert. *Soft: A Software Environment Abstraction Mechanism*. In: USENIX LISA VIII Conference Proceedings, 1994.

[3] FULMER, Robert & LEVINE, Alex. *AutoInstall for NT: Complete NT Installation Over the Network*. In: Proceedings of the Large Installation System Administration of Windows NT Conference, USENIX LISA, Seattle, Washington, USA, 1998.

[4] GOMBERG, Michail & EVARD, Rémy & STACEY, Craig. *A Comparison of Large-Scale Software Installation Methods on NT and UNIX*. In: Proceedings of the Large Installation System Administration of Windows NT Conference, USENIX LISA, Seattle, Washington, USA, 1998.

[5] KIRCH, John. *Troubleshooting and Configuring the Windows 95/NT Registry*. Macmillan Computer Publishing, 1999.

[6] LUERKENS, Cameron D. & COLE, John & LEGG, Danielle. *Software Distribution to PC Clients in an Enterprise Network*. In: Proceedings of the Large Installation System Administration of Windows NT Conference, USENIX LISA, Seattle, Washington, USA, 1998.

[7] *Microsoft Windows NT Workstation 4.0 Resource Kit*. Microsoft Corporation, Microsoft Press, 1996.

[8] SPITZNER, Lance. Armoring NT. Url: www.enteract.com/~lspitz/nt.html

[9] *Srvany.exe. Running applications as services.* Microsoft Press.

[10] *Windows NT Server - Server Operating System. Securing Windows NT Installation.* Microsoft Corporation, Microsoft Press White Paper.

[11] Windows NT C2 Configuration Checklist. Url: www.microsoft.com/technet/security

[12] Windows Knowledge Base. Article ID: Q99885 - *Security Issues that may occur due to the way Windows NT handles FPNWCLNT.DLL*

[13] Windows Knowledge Base. Article ID: 114463 - *Hiding the last logged on username in the logon dialog.*

[14] Windows Knowledge Base. Article ID: 126713 - *Resetting Default Access Controls on Selected Registry Keys*

[15] Windows Knowledge Base. Article ID: 143164 - *How to protect Windows NT Desktops in public areas*