DoIt4Me: a tool for automating administrative tasks on Windows NT networks

Alessandro Augusto, Célio Cardoso Guimarães, Paulo Lício de Geus

IC - UNICAMP
University of Campinas - Campinas, SP, Brazil
alaugusto@yahoo.com.br, {celio, paulo}@ic.unicamp.br

Abstract

The process to secure a Windows NT computer is simple when the system administrator knows the required configuration settings [13,14]. However, even with this knowledge, to apply the same configuration to hundreds of NT-based computers can be frustrating and laborious. Remote administration of a large Windows NT network is a complex task. The tools provided by standard NT installations are, at best, inadequate. The explosive growth in network sizes over the last years has resulted in large and complex sites but no significant new tools were created.

This paper introduces the design and implementation of DoIt4Me, a simple and flexible tool that enables, from a single console, automation of a large number of Windows NT administrative tasks.

1. Introduction

As networked computer systems increase in number of machines and complexity of interconnections, previously simple system maintenance tasks often expand into unmanageable time-sinks. In a wide range of environments, such network administration has become a mission critical task. Organizations are building network in larger scales than ever before, and many are connecting these networks to the Internet without any security concern.

Along with this trend has come an explosion in the use of computer networks as a means of gaining illicit access to computer systems.

With the increased proliferation of system networks, computer security has become an increasingly larger problem for system administrators of large sites (with several hundred or more workstations). Most people would agree that keeping a watchful eye on a handful of workstations is a simple task, but not on several hundred workstations [1, 2].

In an ideal world, every organization would have a system administrator who has enough time, staff and information to plan network growth and security. But in reality, this generally does not happen. System administrators are often responsible for a large number of tasks that keeps them permanently busy and prevents them from keeping themselves up-to-date with new security vulnerabilities and patches [3].

Network victims of any kind of exploit have caused many companies to rethink this model of network security concern. To support the new paradigm, it is necessary to give more attention to the whole network security issue. Security must be maintained not only at the servers, but also on each workstation, i.e. every computer on the network must be made as secure as possible [3].

After a brief introduction, the remainder of this paper is organized as follows. Section 2 describes the motivation for this work. Section 3 reviews some terminology used in this paper. Section 4 shows the design goals that we want in our project. Section 5 introduces DoIt4Me, the tool we developed to automate most of the administrative tasks of a large Windows NT network. Also in section 5, the paper describes some common administrative tasks that DoIt4Me solves for NT environments. Finally in section 6 we make some concluding remarks.

2. Challenges Faced

The Windows NT environment has a reputation to require hands-on, i.e. manual administration. The administrator's physical presence in each machine is necessary every time if configuration is needed. The associated costs increase linearly with the amount of networked computers. Remote software installation and configuration is another problem of this kind of environment [6].

A remote automated procedure should not require that system administrators visit each workstation. This is a problem in many environments where the workstations are located in

different rooms, buildings, towns and so on. Fixing each machine through physically visiting it requires a lot of manpower and can be error-prone; operator errors can lead to machines being configured erroneously, improperly, or not at all.

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 [2]. The automation of system administration and security tasks has been discussed a lot, especially when applied to UNIX-like operating systems. However, solutions derived for the Unix environment are generally not applicable to the Windows NT one.

In a comparison of Windows NT with UNIX systems, NT lacks adequate remote network administration tools [6].

In organizations that have a considerably large Windows NT network, administrators always have a hard time when they need to apply some security configurations on each network machine. These hardships imply on high monetary costs to maintain a group of system administrators in service and normally take many hours of work. The larger a network is, the harder it is to audit, to assess and to maintain compliance of all workstations [1].

Security administration in large Windows NT sites is a very challenging task. In [12] there is a list of the top ten worst security mistakes information technology people make, and the number one is: “Connecting systems to the Internet before hardening them”. Nowadays, there still exist many system administrators who think that the process to apply security on a network is just to install the latest patches. Even worse, there are administrators that install the patches only on the servers' [3].

A large portion of NT security requires modifying Registry values. It seems very difficult to administer NT-based computer networks without expensive administrative tools such as Systems Management Server (SMS) and without a large number of system administrators' [9]. The usual software installation on NT requires the administrator to sit in front of each individual machine, to answer some questions interactively, to wait for the software to load and possibly to reboot the machine. This approach doesn’t scale to hundreds or thousands of NT machines.

So, the challenge faced by us is: (1) to demonstrate the lack of tools to automate most Windows NT administrative tasks; and (2) to present an efficient solution that saves the administrator’s time, effort and budget. We developed this solution, called DoIt4Me: a tool for automating administrative tasks on Windows NT networks.

3. Concepts

It is beyond the scope of this paper to explain all the concepts used, but before proceeding we will clarify some terms. Since its initial release in 1993, the Windows NT operating system appeared as an outstanding operating system with multiple purposes. Designed to integrate client-server networks, Windows NT is divided in two products: Windows NT Workstation and Windows NT Server [10]. During this paper we use the terms workstations, computers and machines as a synonym.

In Windows NT, all configurations are stored centrally in one database called Registry, which is one of the most important system resources, especially when talking about security [8, 10].

The Registry contains all the information about hardware and software configuration: it stores information about user accounts, user groups, and information about installed hardware and software [8].

The Registry is developed in a hierarchical structure and each modification of a Registry’s value directly affects the configuration and the status of that computer.

4. Design Goals

One of the keys to administering large networks is to write tools to handle as many common tasks as possible. This may make it possible to automate common tasks, to spend less time on them, or even to hand them off to other people.

Accordingly, it was also necessary for the purposes of this work to find some way to cover the Windows NT deficiency of tools for remote automation of administrative tasks, and to scale whatever solution to be found to a large number of machines. This had to be done with plenty of configuration flexibility, so as to be tailored to the needs of different machines and administration methods.

Faced with these Windows NT weaknesses, our solution should have some desirable properties:

* Simple use and maintenance
* Centralized
* Scalable
* Configurable in order to meet specific user needs
* Able to provide verification and notification of compliance with security policies
* Capable of enforcing compliance with security policies and standards
* Reduced overall cost of administration
* Inexpensive
* Minimal human interaction

When trying to figure all these desirable properties in a single solution, we decided to implement a new remote system administration tool, called DoIt4Me. Its goal is to automate administrative tasks across a Windows NT network, especially in regards to providing Windows NT remote Registry auditing and configuring in an easy fashion.

5. DoIt4Me

DoIt4Me is an automated, remote administrative tool for Microsoft Windows NT operating systems [1, 3]. It can manage small or large Windows NT networks from a single console. Infrequent trips to distant machines will only be necessary in case of hardware failures.

It is specifically aimed at administrating and securing Windows NT 4.0 machines, although some of the functionality could also be used on Windows 2000.

By installing DoIt4Me on the domain controller (DC), the administrator can remotely control any subset of workstations served by the DC. Implemented in Perl, it can be easily be customized.

5.1 Interface

There is no single interface for configuring and administering an NT network. For example, the audit policy for a standalone NT system is set via the User Manager, while “log specific settings” and all monitoring activities are recorded in the Event Log. Furthermore, each object (file, directory, share, and Registry key) has its own interface for enabling access control lists (ACLs). Rolling out a common audit standard across an NT enterprise and monitoring the Event Logs can be a daunting task [5].

A related issue is whether or not administration tools should be based on a “graphical user interface” (GUI). This kind of interface can be easier to use if the system administrator’s goal is to build or configure a single machine. In general GUI tools are harder to automate and extend. DoIt4Me interface has a simple unified syntax and is used through the NT command line interpreter. Here is an overview of the DoIt4Me interface:

```
C:\> DoIt4Me.pl
---------------------------------------------------------------------
DoIt4Me - Automate NT Administrative Tasks Remotely

Usage: DoIt4Me.pl <option>
Option: <1> Auditing
        <2> Configure the Registry
        <3> Check the status of ALL NT services
        <4> Check the status of subset NT services
        <5> Change NT services status (Start/Stop)
        <6> Reboot a subset of workstations
        <7> Help
---------------------------------------------------------------------
```

5.2 Problems and Solutions

The following problems are time consuming and cumbersome; they requires too much repetitive work, and as such are very error prone. Possible problems include:

Registry Auditing

The first feature of DoIt4Me, is the ability to scan any subset of a network and to report the results for auditing.

In this phase, also called Data Collection, the administrator specifies which configuration settings he or she wants to audit. It is only necessary to specify the subset of machines that will be scanned and the subset of Registry keys that will be collected [1].

As a practical example of remote Registry auditing, suppose the situation where the system administrator needs to know some system information about the workstations. Suppose that the administrator wants to collect the value of the 'DontDisplayLastUserName' Registry key and the version of the Service Pack installed in a subset of workstations. DoIt4Me automates this task making it easy. DoIt4Me only needs to know the subset of the Registry keys and the subset of computers that will be scanned.

Registry Configuring

After auditing, sometimes the system administrator needs to make some adjustments or configure some Registry values to make some computers compliant with the security policy.

DoIt4Me makes configuring the remote Registry as simple as possible. The process is very similar to Registry Auditing, the difference being: in this feature, besides the administrator specifying the subset of computers and the subset of Registry keys, he or she needs to specify the new value that this Registry key will receive. In the above example, if the administrator finds any computer that is not in compliance, he can specify a new value to the 'DontDisplayLastUserName' Registry key and apply it in this option.

Service Status Auditing

DoIt4Me eases the process of getting the status of NT services off remote computers. To perform this action, the administrator needs to specify the subset of computers and the subset of services that he or she wants to audit. There is another function that gets the status of all services. In this case, the administrator needs only to specify the subset of computers intended in the action.

Start/Stop Services

It is also possible to change the status of any service. DoIt4Me allows the system administrator to start or stop any service in any subset of computers. Like the above actions, it is only necessary to define the subset of computers, the subset of services and their new status, for example 1 to start or 0 to stop it.

Applying ACLs

In the current version of DoIt4Me, we are creating a new option to make DoIt4Me apply new ACLs to remote computers.

The are many system administrators that consider their network secure just by installing the latest service pack. As of this writing, the latest service pack for Windows NT is 6a. By just installing it, the system is still vulnerable to some high risk factor vulnerabilities. In [3] we describe a case study of exploring a vulnerability in this category and how to solve it.

Rebooting Workstations

This option allows the system administrator to reboot any subset of computers.

Package Distribution

Some management tasks cannot be performed remotely because of Windows NT limitations, such as remotely accessing some parts of the Registry. Windows systems don't export the whole Registry. Only two of the six Registry keys can be accessed remotely: the HKEY_LOCAL_MACHINE and the HKEY_USERS. The main Registry key necessary to implement security is HKEY_LOCAL_MACHINE, which fortunately is remotely available. But if the administrator wants to modify any Registry value not present in these two keys, DoIt4Me can by-pass this Windows limitation.

In [2], we presented 3 techniques to install distribution packages on Windows NT. These packages contain all changes done to a model machine for replication over the network. For example, the administrator might create a package that contains a new Registry value, one that is not exported by Windows. For more information about how to create these packages, see [2].

After creating the package, the administrator can use DoIt4Me to start the Schedule service on the remote machines. After this, the administrator uses the third technique presented in [2] to schedule a job to install that package on that computer.

With DoIt4Me and the Schedule Technique, the whole Windows NT machine can be modified remotely. In a more general sense, these packages can be used to install or modify any software configuration.

5.3 Reporting

One problem became very apparent during the implementation of this tool. The output produced should be in a format fit for human consumption.

The reports enable the system administrator to identify quickly and easily any problems related to the machines, ranging from a client being down to reporting a subset of machines that are not complying with security policies and standards. What follows is an example of a DoIt4Me report of a Registry auditing, where the subset of computers is: {porsche, mustang} and the subset of registry keys is: {CSDVersion, DontDisplayLastUserName}. The report looks like:

```
C:\> DoIt4Me.pl  1
-------------------------------------------------------------------------------
                              Auditing Report
-------------------------------------------------------------------------------

COMPUTER         KEY                          VALUE
---------------  -------------                -------------
mustang          CSDVersion                   Service Pack 6
porsche          CSDVersion                   Service Pack 5

mustang          DontDisplayLastUserName      0
porsche          DontDisplayLastUserName      0
```

6. Related Work

Harlan Carvey presents in [4] a framework of a few administrative scripts that had some similar goals to our project's. For example, one of his scripts, called 'regkeys.pl', is devised to collect Registry values from a remote NT system. However, these scripts have some weaknesses: they are not scalable to a large NT network.

As a practical example of remote auditing and compliance, if the system administrator wants to collect the value of the 'DefaultUserName' Registry key of all workstations, it could be done with the script presented by Harlan, but the administrator will spend a lot of time and effort. It requires human intervention for each audited machine. The administrator will have to execute the script for each computer. The script audits only one computer at a time. The effort to compare the results after all executions is really hard too.

It is clear that his approach is unable to handle a large number of machines. Also, once the system administrator knows which workstations are not in compliance with security policies, there is no ability to configure the machines with new values, i.e. to act upon.

However, these scripts also have their strength, since they show how to do the remote collection for a single machine, and as such can be used as a building block to achieve our goals.

7. Conclusions

Security administration in large NT sites is a challenging task and it is imperative to automate it as much as possible. This requires a combination of auditing, assessment and compliance mechanisms. Most of the tools available today focus on the identification of security vulnerabilities, not on their correction.

The cumbersome task of automating administrative tasks can be easily done with DoIt4Me. The current version of DoIt4Me addresses security weaknesses and eases standardization and adherence to NT network security policies. Our experience has confirmed that it is possible to remotely manage a large NT network in a scalable way with DoIt4Me.

By automating the system administration tasks, we achieve several gains. Firstly, we eliminate error-prone repetitive tasks. Secondly, the tasks are done in a timely fashion, saving computer and staff resources. Finally, the system administrator can customize DoIt4Me's code at any time.

With the introduction of DoIt4Me, this paper has described a solution to many problems faced in managing Windows NT networks.

8. References

[1] AUGUSTO, Alessandro, GUIMARAES, Célio and de GEUS, Paulo Lício. "Administration of Large Windows NT Network with DoIt4Me". Proc. of SANS'2001, the 10th International Conference on System Administration, Networking and Security, Baltimore, MD, USA, May, 2001 (accepted).

[2] AUGUSTO, Alessandro, GUIMARAES, Célio and de GEUS, Paulo Lício. "Administration Techniques for Implementing Security on Large Windows NT Networks". Proc. of SSI'2000, the 2nd Symposium on Informatics Security, S. José dos Campos, SP, Brazil, 24–26/10/2000, pp 1–10.

[3] AUGUSTO, Alessandro, GUIMARAES, Célio and de GEUS, Paulo Lício. "Service Packs are not the Panacea of Windows NT Security". USENIX-LISA-NT'2001, the Large Installation System Administration of Windows NT Conference (to be submitted).

[4] CARVEY, Harlan, "System Security Administration for NT". Proc. of USENIX LISA-NT'1999, the 2nd Large Installation System Administration of Windows NT Conference, USA.

[5] COX, Phil. "Auditing: The Ugly duckling of Computers". ;Login: The Magazine of USENIX & SAGE, 1998.

[6] GOMBERG, Michail, EVARD, Rémy and STACEY, Craig. "A Comparison of Large-Scale Software Installation Methods on NT and UNIX". Proc. of USENIX LISA-NT'1998, the Large Installation System Administration of Windows NT Conference, Seattle, Washington, USA.

[7] GOMBERG, Michail, STACEY, Craig and SAYRE, Janet. "Scalable, Remote Administration of Windows NT". Proc. of USENIX LISA-NT'1999, the 2nd Large Installation System Administration of Windows NT Conference, USA.

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

[9] LUERKENS, Cameron D., COLE, John and LEGG, Danielle. "Software Distribution to PC Clients in an Enterprise Network". Proc. of USENIX LISA-NT'1998, the Large Installation System Administration of Windows NT Conference, Seattle, Washington, USA.

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

[11] ROTH, Dave, "A Networked Machine Management System". Proc. of USENIX LISA-NT'1999, the 2nd Large Installation System Administration of Windows NT Conference, USA.

[12] SANS. "Mistakes People Make that Lead to Security Breaches". 2000. http://www.sans.org/mistakes.htm

[13] TCSEC Final Evaluation Reports. TTAP-CSC-FER-99/001. Microsoft Corporation, Windows NT Workstation and Windows NT Server, Version 4.0. http://www.radium.ncsc.mil/tpep/library/fers/TTAP-CSC-FER-99-001.pdf

[14] Windows NT C2 Configuration Checklist. http://www.microsoft.com/technet/security