BY SUSAN EISENHARD

Windows 2000 Secondary Logon

Addressing the Security Risks of the Network Administrator's Account

Today's network administrators must protect their systems from hackers. One tool that can be used to thwart this type of attack is the Windows 2000 Secondary Logon. This facility allows the network administrator to use a "normal," less powerful network account to perform non-administrative functions. When an administrative function must be performed, the network administrator can run the selected utilities using a privileged network account. All this can be done without logging out and back into the network.

The following story is purely fictitious. The people, organization and events discussed in this story are all fictitious. No association with any real people, organizations or events is intended or should be inferred.

A cute little animated electronic greeting card is circulating through the internal email boxes within an organization. It is such a cute card that it spreads through the organization within a few days. As you walk down the hall, you can hear people talking about it: "Did you see that greeting card? It was so cute! It's the most clever electronic greeting card I have ever seen!" Little did they know, but this greeting card was much more clever than anyone had yet realized. A hacker developed this greeting card. The hacker was not content with simply destroying a few files on the victim's PC; he wanted to destroy as much data as possible. This meant attacking the corporate file and application servers. In order to wreak as much havoc as possible, the destructive code buried within the greeting card waited until it was run under the account of a network administrator. The "normal" network user would simply be shown a cute little animation, but when run under an administrator account, the destructive code was unleashed. The data and programs on multiple file servers' drives were destroyed. Then the code would go out to these same servers and cause them to crash. Needless to say, the servers would not come back up until a system restore was performed. To be even crueler, the code buried itself within the network administrator's PC so it could wreak its havoc again a few days later.

The Windows 2000 Secondary Logon service helps ease the pain associated with the use of multiple accounts by not requiring the network administrator to logout then back into the network when he needs to perform administrative tasks.

As you read that story, did you get a sinking feeling in your stomach? Have you ever opened an electronic greeting card or other "amusement" type email attachment using an administrator level network account? Never underestimate a hacker. One of the primary responsibilities of today's network administrator is to protect the company they work for from hackers. In order to help protect your network from a hacker, you need to think like a hacker and then implement tools and policies that would thwart the hacker's attacks.

One of the tools you can use to help thwart this type of attack is the Windows 2000 Secondary Logon. The Windows 2000 Secondary Logon facility allows the network administrator to use a "normal," less powerful network account to perform non-administrative functions. When an administrative function must be performed, the network administrator can run the selected utilities using a privileged network account. All this can be done without logging out and back into the network.

Now I realize that many of the network administrators who are reading this are saying to themselves, "Oh boy, here we

go again. Someone is always wanting to take away the network administrator's account privileges." Well, it is time to change this mindset. Most organizations are now connected to the Internet. Viruses and Trojan horse attacks are the way of the world today. It is your responsibility to help protect your organization from these threats.

Many organizations have already restricted access to privileged network accounts. The network administrator is given a user-level account with limited rights and security to perform non-administrative functions. When the network administrator needs to perform privileged functions, he is required to logoff, then log back on to the network using an administrative level account. Windows 2000 Secondary Logon provides a method to achieve this same objective without requiring the network administrator to logout and back into the network. This function is also known as the "RunAs" service.

STARTING THE RUNAS SERVICE

The default Windows 2000 Server and Windows 2000 Professional installation enables the RunAs service to start automatically. Before you begin to test and work with the RunAs service, you should check to make sure that it is in fact running on your systems. To check the status of the RunAs service, perform the following: Start > Settings > Control Panel > Administrative Tools > Computer Management > Services and Applications > Services. You will see a screen similar to the one shown in Figure 1. Notice that in this example, the RunAs service is running. The RunAs service also has a Start Up type of Automatic, causing the service to start each time the machine is re-booted.

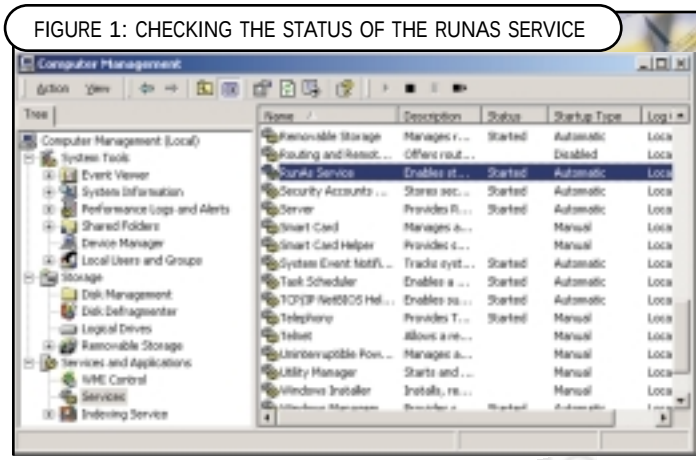
TESTING THE RUNAS SERVICE

The best way to see how the RunAs service works is to try it. Set up a "normal" network or local machine account. If you are currently using Active Directory, you should create a new user within Active Directory. This account should not have any special security or privileges associated with it.

From your Windows 2000 computer, login using the new non-privileged account. Try to run a privileged application, such as viewing the Security Event log using the following command: Start > Settings > Control Panel > Administrative Tools > Computer Management > Event Viewer > Security. You should be denied access and receive the message shown in Figure 2. Now try the following:

1. Click on Start > Settings > Control Panel > Administrative Tools. You should see the icon for the Computer Management application within the Administrative Tools folder.
2. Hold down the Shift key, and right-click on the Computer Management icon. You should see the menu shown in Figure 3.
3. Select the "Run As" menu option, and the "Run As Other User" dialog box will be displayed, as shown in Figure 4.
4. Enter a privileged account and password, and you should now be able to view the Security Event log. In this example, I entered the credentials for the Administrator account.

FIGURE 1: CHECKING THE STATUS OF THE RUNAS SERVICE



CREATING A SHORTCUT TO USE THE RUNAS SERVICE

Another method for using the RunAs service that is a little less cumbersome is to set up shortcuts that use RunAs on your desktop for the privileged applications that you use on a daily basis. To do this, perform the following steps:

1. Create a New folder on your desktop named "Privileged Applications."
2. Copy the "Computer Management" icon (or other privileged application icon) into this folder.
3. Select the new icon with a single left-click.
4. Right-click on the icon and then select Properties. The screen shown in Figure 5 will be displayed.
5. Click to enable the "Run as different user" selection, and then click on OK. When you double-click on the new icon, you will receive the "Run As Other User" dialog box shown in Figure 4. Enter the account information of a privileged user, and you are on your way.

Note: Each time you use this new shortcut, you will have to enter the account information of a privileged user. This is a bit more difficult than simply using a privileged account all of the time, but this small sacrifice can greatly enhance the security of your network. Another feature of the RunAs service is that it requires you to enter the privileged account credentials each time you use it. This prevents an unauthorized user from attempting to run privileged applications from your PC if you leave it unattended (this happens more than you may think!).

USING THE RUNAS SERVICE FROM A COMMAND PROMPT

You can also invoke the RunAs service from a command prompt. To do this, open a Command Prompt, or click on Start > Run and enter the following, where xxx.xxx is the name of a program:

```
runas /user:username xxxx.xxx
```

For example, to start Notepad.exe under the administrator account, enter the following:

```
runas /user:corporate\administrator notepad.exe
```

FIGURE 2: ATTEMPTING TO RUN A PRIVILEGED APPLICATION USING A NON-PRIVILEGED ACCOUNT

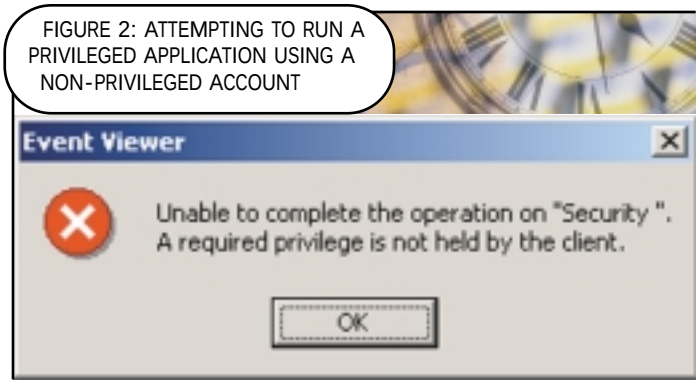


FIGURE 3: ACCESSING THE RUNAS COMMAND

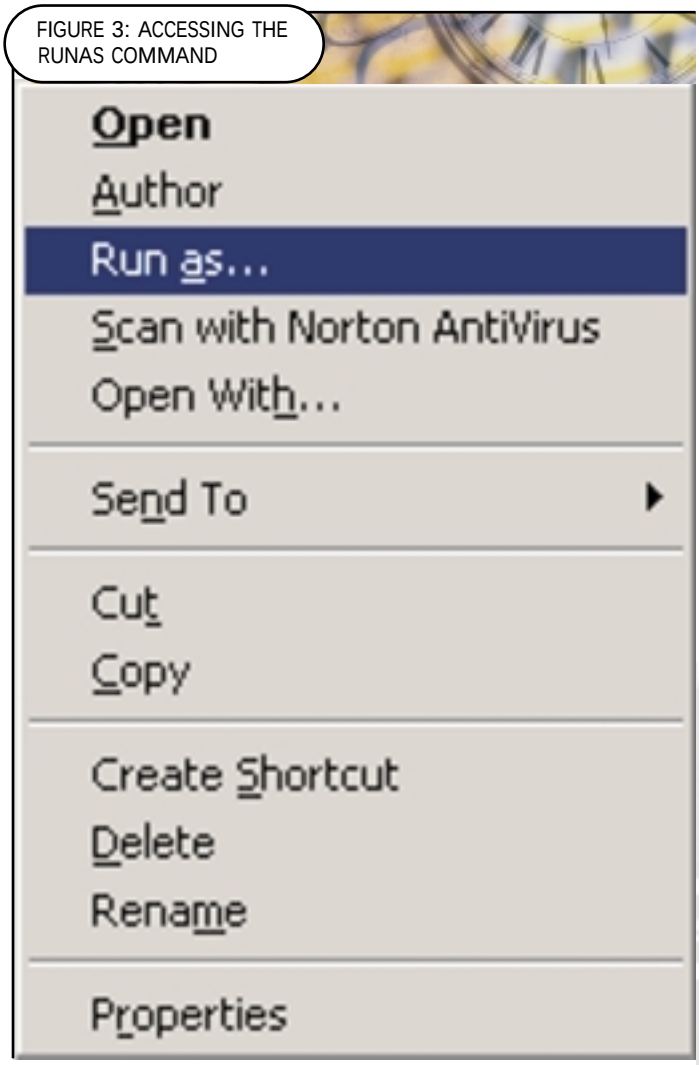


FIGURE 4: ENTER THE PRIVILEGED ACCOUNT CREDENTIALS

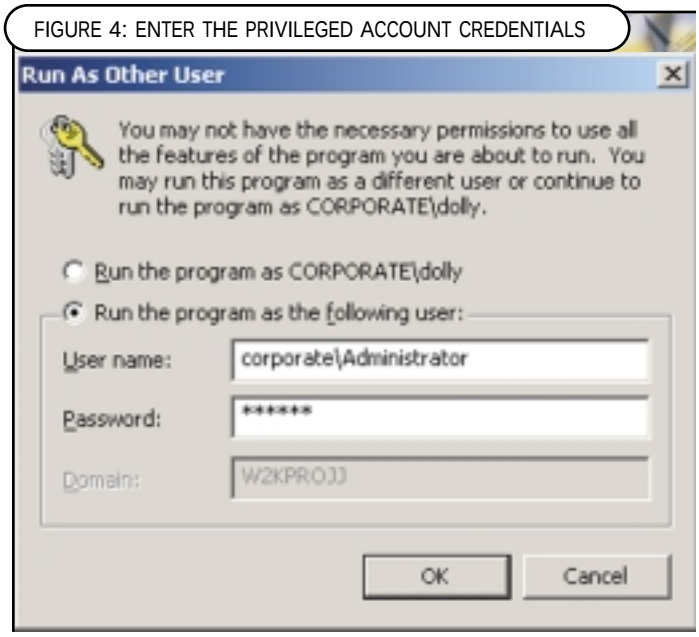
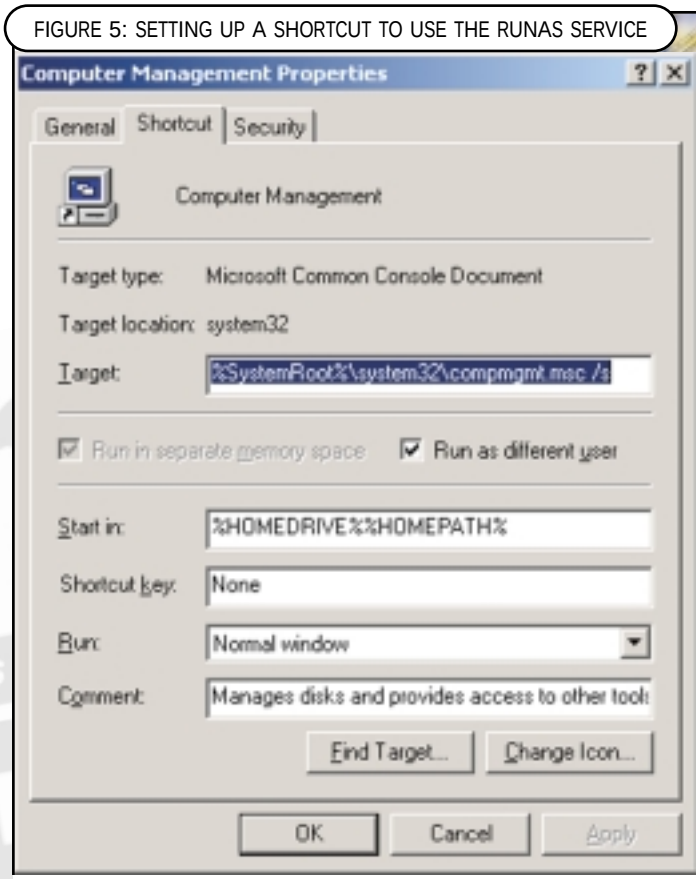


FIGURE 5: SETTING UP A SHORTCUT TO USE THE RUNAS SERVICE



You will be prompted to enter the password of the Administrator account.

CONCLUSION

Many network administrators have full privileges on all the file servers within their employer's network. Many of these same network administrators also have full access to all of the files systems associated with these servers. This is a disaster just waiting to happen. Nobody would deny that a company must trust their network administrators and that they require certain high-level access privileges. Nevertheless, it just makes common sense to use this high-level access only when required. The Windows 2000 Secondary Logon service helps ease the pain associated with the use of multiple accounts by not requiring the network administrator to logout then back into the network when he needs to perform administrative tasks.

I realize that many of you are cursing me for writing an article that addresses the security risks of the network administrators' account. Trust me, if you take steps to implement technologies such as the Windows 2000 Secondary Login to protect your company's

network resources, you will look like the hero. You may also save yourself the embarrassment of having to explain why a Trojan horse attack launched from your network account destroyed your companies' data.

Susan Eisenhard is a project manager for a major East Coast software development company. Susan is also a small business entrepreneur. She owns a physician billing company, a small accounting business and is currently starting a new Internet-based publishing company. Susan can be reached at susiee@fast.net.