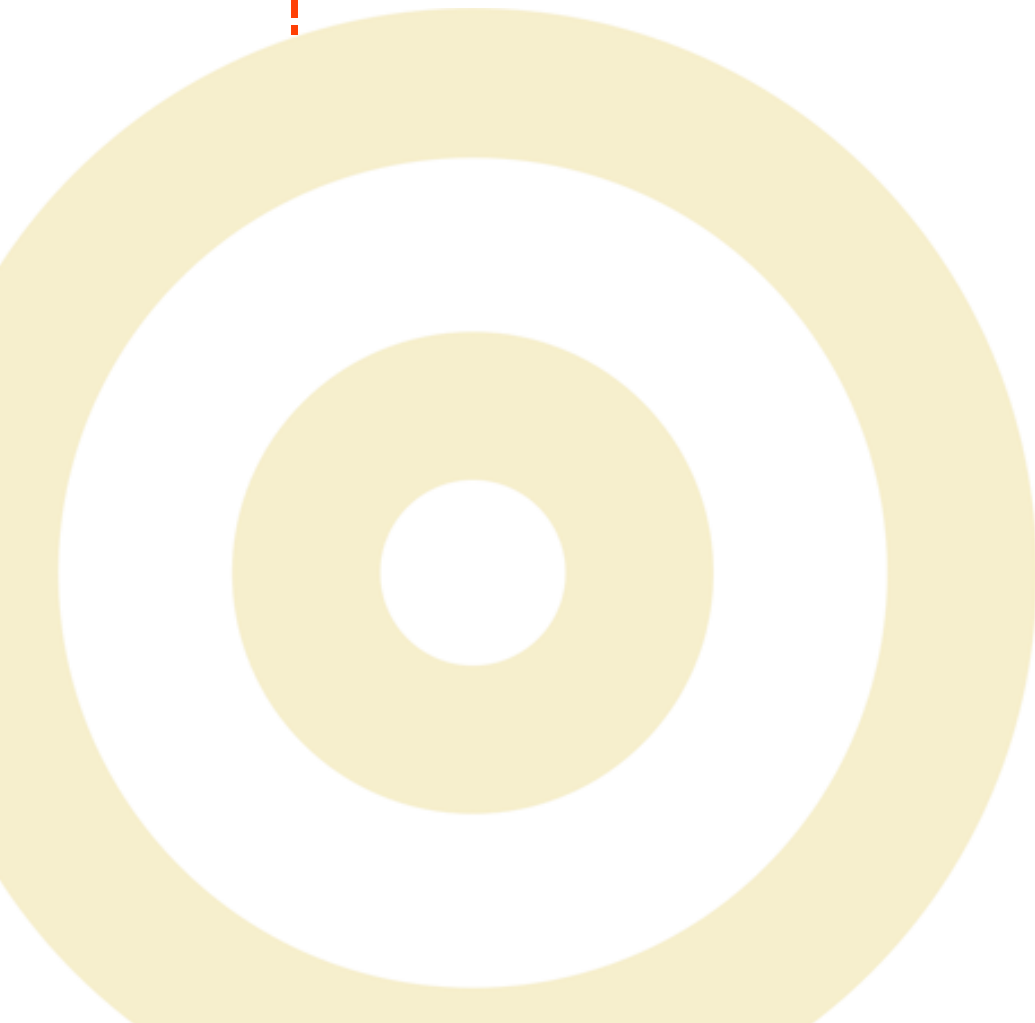


Securing Terminal Services



Sponsored By:



Securing Terminal Services

By Christa Anderson

© 2004 TechTarget

BIO

Christa Anderson—Christa is a SearchWin2000.com resident site expert on terminal services and is an internationally known speaker and writer on server-based computing. Her books include *Windows Terminal Services*, *The Definitive Guide to MetaFrame XP*, and she is the co-author of the best-selling *Mastering Windows Server 2003*. Sign up for her email newsletter at www.termservhub.com.

This *IT Briefing* is based on a Wyse/TechTarget Webcast, “[Securing Terminal Services](#).” To view this Webcast online, please click the link.

This TechTarget *IT Briefing* covers the following topics:

- How is server-based computing more secure than client-based computing? 1
- What security issues does server-based computing introduce? . . . 2
- What parts of the computing infrastructure need to be secured? . . 2
- What are some approaches to securing this infrastructure?. 2
- Line security 5
- Connection security 6
- Common questions 7

© 2004 Wyse Technology Inc. All rights reserved.

About Wyse Technology Inc.

Wyse Technology offers end-to-end server-centric access solutions for Web- and Windows-based applications. Its award winning line of secure, managed, affordable, and reliable Wyse Winterm thin clients have made Wyse the worldwide leader in thin clients for the past seven years. Our industry-leading remote management software helps organizations reduce costs, mitigate security risks, and improve worker productivity. With Wyse Winterm thin clients, you can choose from a variety of operating systems including Microsoft Windows CE, .NET, Microsoft Windows XP Embedded, and Linux. Visit www.wyse.com, and learn how thin clients can help your organization.

About TechTarget *IT Briefings*

TechTarget *IT Briefings* provide the pertinent information that senior-level IT executives and managers need to make educated purchasing decisions. Originating from our industry-leading Vendor Connection and Expert Webcasts, TechTarget-produced *IT Briefings* turn webcasts into easy-to-follow technical briefs, similar to a white paper.

Design Copyright ©2004 TechTarget. All rights reserved.

For inquiries and additional information, contact:

Tina Hills

Director of Product Marketing, Webcasts, TechTarget

thills@techtargt.com

Securing Terminal Services

How is server-based computing more secure than client-based computing?

The terminal services model carries many administrative benefits. However, terminal services does involve security issues that don't enter into client-centric computing. You have to worry about who is running what on the terminal servers, whether users are licensed for those applications, whether the communications between server and client can be intercepted, and whether users can copy sensitive information to their home computers. This white paper examines some of the approaches to closing security holes in server-based computing.

As shown in Figure 1, server-based computing is more secure than client-based computing in several regards. The main thing is the data never leaves the server. With server-based computing, you are running applications on the server and displaying them on the client, but the data isn't there. The only thing that happens on the client side is any user input that is made through keystrokes and mouse clicks. This means the data never has to leave the secure office (although depending on the way you've set it up, it may be visible for non-secured locations). It also means that you are not depending on clients to back up their computers. Those who have tried maintaining a peer network node know that relying on individuals to back up desktops is asking for trouble.

How is server-based computing more secure than client-based?

- Data never leaves the server
 - does not have to leave the secure office (although may be visible)
 - you're not dependent on clients to back up their computers
- Possible to use thin clients
 - useless without a terminal server
 - not often vulnerable to viruses
 - generally speaking, no way to save data locally

Figure 1

It is possible to use thin clients with server-based computing. The thin clients are useless without a terminal server, however, which means no one can walk off with them. Another feature of thin clients is they are not generally vulnerable to viruses. For thin clients, there is no way to save data locally. This can be a major advantage in the case of a physical security breach.

What security issues does server-based computing introduce?

Figure 2 lists a few challenges of server-based security. One difficulty is that one person's error can impact dozens of people. In effect, many people are sharing the same workstation, i.e., the terminal server. This is one major reason not to use domain controllers at terminal servers.

Now one issue related to having multiple people logging onto the same server is that Windows by default leaves everything unlocked. This is somewhat less true in Windows 2003 than it is in Windows 2000, but it's still true to a fairly significant extent. Publish-

ing single applications does not secure the desktop (though some are under the impression that it does), but if users can only see an application they can't get to know anything else. Some applications also provide easy access to the file system and users can email applications to themselves. This certainly runs counter to the goal of closing all the server-side security holes.

What parts of the computing infrastructure need to be secured?

You should take a three-tiered approach to locking down server-based computing. The first tier is to secure the server. Next is to secure the connection between client and server. The third prong is to secure the client.

What are some approaches to securing this infrastructure?

Regarding server security, the first step is to restrict login access to the terminal server (see Figure 3).

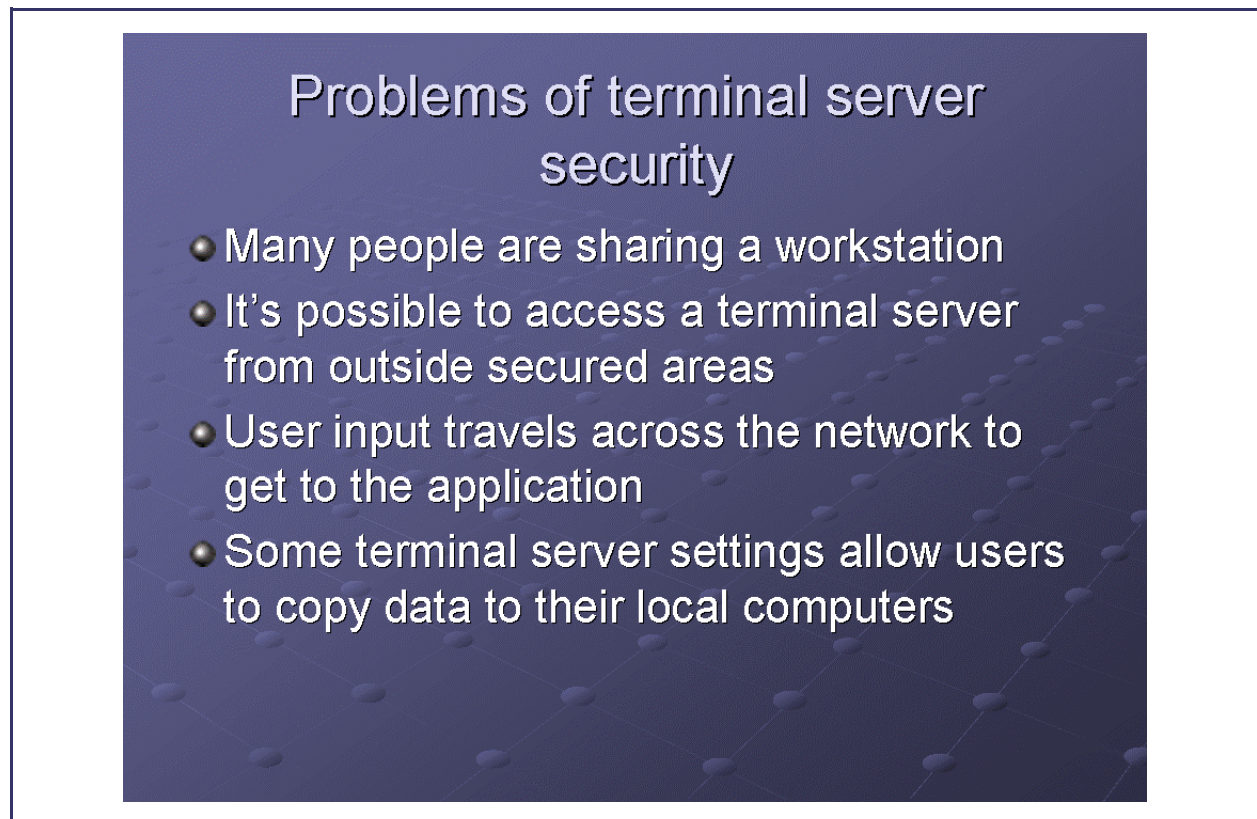


Figure 2

Restricting Logons

- By default, all users can log onto the terminal server
- Providing terminal-only logins
 - give different permission sets for remote connections
 - some tools allow for restricting access based on terminal used for login

Figure 3

Once people are on the terminal server it is important to restrict folder access. Once they are in the folders they are allowed to access, you must prevent unauthorized applications from executing.

In Windows 2000 and 2003, all users by default have the right to login to the terminal server. In Windows 2000 you can fix that only on a per-user basis by opening up the property dialog box and disabling that login. In Windows 2003 you can use policies to disallow logins for organizational units. By now, most administrators have installed the licensing fix that came after Service Pack 2 for Windows 2000. But before this licensing fix was applied, when people connected to the terminal server their computer was given a license, even before they successfully logged on. And because of this, it was very easy to grant licenses to people who never should have had them in the first place. Therefore, it is very important to install this licensing fix.

When you are restricting logins, some third party software also gives you the ability to restrict access based on what terminal they are using as opposed to who they are, as well as giving different permission sets based on which computer they are using.

There are a couple of different ways to restrict access to the terminal server. First, we can prevent individuals and machines from logging on. Depending on who that machine belongs to, we can also restrict what the user does or what kind of access he has. You can use the software restriction policies in Windows XP to immediately restrict user access to the terminal server.

Once the user is on the terminal server, you'll need to restrict access to folders there (see Figure 4). When you are installing terminal services, there is a section in which you are asked what security settings you want to have. However, the wizard doesn't really explain what this means. Windows NT on the other hand allows modification of files in system folders. This is done for backward compatibility with applications that want to write to INI files stored in the system directory.

Generally speaking, you don't want to give users the ability to modify any content in the system directory. What you can do instead is to modify permission on per-application folders or files, so they only have modified permission on the folders they need as opposed to the whole thing. If you want to make sure

Restricting Folder Access

- Windows Server security vs. NT-compatible security
- Restricting access to per-user My Documents

Figure 4

users have access only to the My Documents folder, that will keep them from having access to other folders and subfolders.

Preventing unauthorized applications from running is a bit more complicated (see Figure 5). As mentioned, you don't want users to run every application they can get to even if the application is installed on purpose on the terminal server. You may not have licenses for everyone to run that application. It is possible that a terminal server could be infected with a virus. A user could potentially download and execute malicious software. Some software you don't want people to run because it is resource-intensive even if it is not malicious.

In Windows 2000, you use user-group policies to prevent unauthorized applications from running. It is possible to lock down the user environment, which means not just controlling which applications are executed, but also controlling whether or not people have access to run the taskbar or anything else from the operating system. However, this requires enabling and setting 32 separate policies and you need to get all of them.

Group policies apply mainly to users, not to machines, and even when they do apply to machines they apply to the terminal server. They do not apply to the client computers, so if you have a setup that requires that people only use an application if they are logged in at a certain terminal, that will not be an option using group policies. And of course using group policies will require Active Directory. Although Active Directory has been available for some years, many companies are only just beginning to roll it out.

Windows 2003 has group policies and some additional features to make tuning a bit easier. It also has something called software restriction policies, separate from the group policies, that improve the per-application restrictions. These policies prevent applications from executing, regardless of what process they are launched from. Its policies are a "white list" or "black list" model. White list means you provide a list of applications that are allowed to execute on that terminal server. Black list means you provide a list of ones that are not allowed to execute. Software restriction policies are only available for Windows Server 2003 terminal servers.

Preventing Unauthorized Applications from Running

- You don't want users running every application they can get to
 - unlicensed software
 - malicious software
 - resource-intensive software
- Group policies
- Software restriction policies
- Process-specific restrictions

Figure 5

In setting up a terminal server, it is to your advantage to start with nothing and then apply selectively as opposed to starting with everything. If you start with nothing you know exactly what has been given to the users. You don't have to worry about what they might have that you don't know about.

Line security

There are three different types of line security: display protocol encryption, wireless networks, and protection for outside connections. For display protocol encryption, you can use both RDP (which is used by Windows Terminal Services) and ICA (which is used by MetaFrame) and all versions of MetaFrame support encryption. The level of encryption governs the level of encryption between client and server. In RDP, for example, the default level of encryption is medium, which means that all communications between and client and server are encrypted with a 40-bit algorithm (if you are using an operating system prior to Windows 2000) or 56-bit (if the client is running Windows 2000 Professional or XP Professional). Low encryption covers only the initial login, namely the password, and not if the user has passed through after the connection is made.

Just doing protocol encryption may not be enough, however. If you use wireless networks, you should also use wireless encryption. You should also create a white list of MAC addresses that are allowed to use the network. If you do that, people who are not permitted to get on the network generally don't have the skills to get on.

Workers outside the office might access the network through a virtual private network or with SSL. Currently only ICA supports SSL. SSL is best for securing connections to people when you can't be sure what computers they will be using. It enables you to have a secured session where the user is logging in from a hotel computer, a terminal, a laptop—it really doesn't matter what machine they are working from or even which IP address they have.

VPNs are better for when you know which computer is permitted and need a more secure connection. For example, if you want to know that someone is using a certain machine, has a static IP address, or it is going to be a certain IP address.

Connection security

As for client security, in Windows 2003, RDP now supports drive mapping. This is not true in earlier versions of Windows Terminal Services. Drive mapping is convenient but it means you now have access to the locally driven hard drives on a client computer, so people can copy data and put it on their client computer. For this reason, drive mapping is not enabled by default on the client. To turn it on you will need to enable it actively. You can also disable this capability on the server side, which you would want to do if you have sensitive data that you can't afford to have stored on someone else's hard drive. Another option is disabling clipboard mapping.

Normally speaking in RDP and ICA, it is possible for users to test in a terminal session and copy it to their local session or vice versa. If you do that, then you will have the document once you save it. If you are trying to make sure the data cannot leave the terminal server and you want to disable clipboard mapping, once again that can be done on the server on either a per-user or per-protocol basis.

Although it is possible to include the user login to automatically login to the terminal or with ICA to pass through authentication, it is a good idea to disable that option. Although it is more convenient for the user it does set the stage for foul play if someone leaves their desktop unattended. Then someone could login to the terminal server without having to know any login. Once they are on the terminal server, they implicitly have access to the network.

In summary, terminal services can be more secure than client-centric computing because you have better control over where the data is stored. But the shared environment does introduce new issues to worry about. When addressing these issues, you will need to balance the security of your environment against inconvenience to the users. It is simpler to allow drive mapping and it is simpler to allow keyboard mapping, for example. If you disable those you may hear about that from the users. On the other hand it depends somewhat on the degree of security you need to have for your data.

Common Questions

Question: If an enterprise has only one server, why should domain controllers not be terminal servers?

Answer: For viability reasons, you don't want anyone working on the terminal server and doing something that takes down the terminal server, not only taking down everyone else's workstation but also taking down the domain controller. This is less of a problem now than it used to be because there are a number of tools for managing print drivers. But it is possible for a print driver to take down the terminal server. Say, for example, someone is printing, those print drivers are not supported in the terminal server and the server blue-screens. At that point we have taken down not only everybody who is working on that terminal server but also any functions the domain controller should be handling. That means no one can authenticate until the domain controller comes back up, and if an enterprise only has one server, it only has one domain controller. This is not a recommended approach.

Question: I am concerned about usage of my software via Terminal Services beyond what I licensed it for. The licensing software I use attempts to tell you if you are using Terminal Services but I don't think this will work correctly in all configurations.

Answer: Most applications don't have good license metering built into them. Being able to determine who is launching the application, who is running it, and prevent that based on user identity would be a step in the right direction.

Question: Are there any benefits to using Windows Server 2003 versus Windows Server 2000 in terms of terminal services?

Answer: On the client side, you have drive mapping, you have greater color depth, you have a faster connection. It is much snappier now than it has ever been even with more features enabled. On the server side, what really makes it more usable is the addition of group policies for managing terminal server settings. In Windows 2000, you have to configure termi-

nal server settings either on a per-protocol basis, which means for everybody using RDP, or on a per-user basis. None of these settings were exposed to WMI so you couldn't access them through administrative scripting. If you want to configure remote control settings on a per-user basis, for example, you need to open each user's properties and go through the configuration. The major differences in Windows Server 2003 are a richer client experience for users and somewhat better administration on the server side.

Question: Is there a central source for obtaining or identifying approved drivers since they always seem to be a problem?

Answer: When it comes to printer drivers, anything that's included with the operating system is approved. However, you can't count on a driver being included with the operating system because new printer drivers come out all the time. What you need to do instead: use driver management tools (like those that are available with MetaFrame) and other third-party tools. Then, test your drivers. Make sure they work and then distribute them to terminal servers so they are pre-installed. Another option is to avoid the problem altogether using the universal printer drivers available with MetaFrame. Universal printer drivers are not in fact universal, they are just relatively flexible. They are meant to work with most printers. They will give you up to a certain degree of resolution, up to a certain degree of color. If you need a more complete solution that avoids the universal printer driver, you could use virtual printer drivers.

Question: What thin clients have you found to work best?

Answer: Wyse now offers a wireless thin client that is easy to carry around. Thin client selection criteria include a small form factor, flexibility, and good management software on the client. The whole point of using thin clients is to make the environment easy to manage. The client's management software is an important part of that.

Question: Are there any known security threats designed specifically for terminal service?

Answer: There have been reports of some denial-of-service attacks against port 3389 and port 1494, which is one reason you don't want it accessible to the outside world.

Question: Does Terminal Services support individual application publishing?

Answer: Yes, to some degree. What you can do is set up the Terminal Services session so it displays only a

single application. However, if the window is not identified as an individual application, it still identifies an RDP session.

Question: Is there any easy way to check and/or switch security compatibility mode in terminal service?

Answer: Yes, you can check at the terminal server's configuration; the information is exposed there. It will indicate Windows 2000-compatible security, legacy security, NT security. To change that, you may need to reinstall the service.



About TechTarget

We deliver the information IT pros need to be successful.

TechTarget publishes targeted media that address your need for information and resources. Our network of industry-specific Web sites give enterprise IT professionals access to experts and peers, original content and link to relevant information from across the Internet. Our conferences give you access to vendor-neutral, expert commentary and advice on the issues and challenges you face daily. Practical technical advice and expert insights are distributed via more than 100 specialized e-mail newsletters, and our webcasts allow IT pros to ask questions of technical experts in real time.

What makes us unique

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals. We leverage the immediacy of the Web, the networking and face-to-face opportunities of conferences, the expert interaction of Webcasts and Web radio, the laser-targeting of e-mail newsletters and the richness and depth of our print media to create compelling and actionable information for enterprise IT professionals. For more information, visit www.techtarget.com.

Wyse Technology offers end-to-end server-centric access solutions to Web- and Windows-based applications with our award-winning line of Wyse® Winterm thin clients and remote management software. Visit <http://www.wyse.com> and learn how thin clients can help your organization.

WYSE_0003_07/2004