Global Information Assurance Certification Paper

Tony Sweeney
Version 1.2e
July 1, 2001

Using Microsoft Terminal Services and Windows Terminals to Protect Confidentiality, Integrity, and Availability.

Introduction

With distributed PC-based computing, much of the organization's resources are spent supporting end-user hardware and PC configuration issues. Using Terminal Services, the administrator will have the time and resources to focus on security. Terminal Services with Windows terminals is the most secure configuration but also has a range of technical, educational, cultural, political, and internal marketing challenges.

Terminal Services and Windows Terminals is a server-based computing environment. The following description of Windows NT Terminal Server is given as:

> Terminal Server is an extension of the Windows NT Server 4.0 product line. In the multiuser environment, a terminal emulator displays the Windows desktop operating system and runs Windows-based applications completely off the server.
>
> Windows NT Server 4.0, Terminal Server Edition, has a multi-user server core that provides the ability to host multiple, simultaneous client sessions on Windows NT Server 4.0, and on future versions of Windows NT Server.
>
> - A new class of low-cost hardware, commonly referred to as Windows-based terminals, marketed by third-party hardware vendors. A Windows-based terminal contains an embedded terminal emulation client.
> - Any existing 32-bit Windows desktop operating system, such as Microsoft Windows 98 or Microsoft Windows NT Workstation (running the terminal emulation client as a window within the local desktop environment).
> - Older 16-bit Windows-based desktops running the Windows 3.11 operating system (running the 16-bit terminal emulation client as a window within the local desktop environment).
> - X-based terminals, Apple Macintosh, MS-DOS, networked computers, or UNIX-based desktops via third-party, add-on products.
>
> Terminal Server is capable of directly hosting compatible multi-user Windows NT client desktops running on a variety of Windows-based and non Windows-based hardware. Standard Windows-based applications do not need modification to run on Terminal Server, and all standard Windows NT-based management infrastructure and technologies can be used to manage the client desktops. (Cumberland, Brian, Carius, Gavin, and Muir, Andrew. p.xxi)

A Windows-based terminal (WBT) is described as:

> The term Windows-based terminal broadly describes a class of thin client terminal devices that can be used to gain access to servers running a multi-user Windows operating system, such as Terminal Server "(Cumberland, Brian, Carius, Gavin, and Muir, Andrew p.155).

Windows terminals are available from a variety of manufacturers with most having no moving parts and the operating system stored on ROM. The Windows terminal that will have the lowest TCO, be easiest to manage, and be most secure should only run remote applications and have no local peripherals or local file sharing. To limit configuration-related problems, the Windows terminal should lockout the local user from changing the configuration settings once set. If the copying of sensitive data is an issue, the availability of drives, printers and the Windows Clipboard can be restricted. Another layer of security is provided with Windows-based terminals that use Smart Card hardware-level security. To use the terminal the user must have a card and possess a PIN [Personal Identification Number]). Also, choose a vendor that provides tools that will enable administrators to manage and upgrade the flash ROM from a remote server.

Security Policy

With the administrator spending less time supporting end-user hardware and PC configuration issues, they should have time to write and evaluate an effective and usable security policy. This policy should include how the servers and Windows terminals are configured to insure the highest level of protection. An anti-viral policy is probably the most important part of any security policy. In today's environment viruses spread very quickly and it's important to know where to go to get information on whether it is a virus or a hoax. In addition, the anti-viral policy should include the steps to be taken to keep the anti-viral signatures up to date.

Securing the Server

Of course, the servers have to be secure electronically as well as physically. If physical access is not enforced, all the other security measures taken will have limited effect. Physical security is the first line of defense in protecting a server. The goal is to protect the file system and registry from attack. This should prevent unwanted users from accessing the server and prevent valid users from accessing information or areas they shouldn't be accessing. A properly secured server prevents data loss and system corruption. Some resources available in securing Terminal servers are:

(1) CITRIX MetaFrame for Windows Terminal Services.
(2) Configuring Citrix Metaframe for Windows 2000 Terminal Services.
(3) http://www.sans.org/newlook/publications/ntstep.htm
(4) http://www.secadministrator.com/Articles/Index.cfm?ArticleID=16524&Key=Permissions

Modems

The modem is the weak link on a secure network. With modems on the network, a firewall can easily be subverted. The two biggest problems are attackers scanning modems using telephone scanners called "war dialers," and attackers scanning the network while connected to the Internet. An administrator's worst nightmare is an employee with an unauthorized modem on his desktop PC, who installs a remote-control program such as pcAnywhere (without a password), and turns on the modem before going home at night. The first and most obvious step to take to prevent the installation of unauthorized modems is to specifically prohibit them in your enterprise security policy. While this step should eliminate most unauthorized modems from your networks, it surely won't get rid of all of them, particularly in companies with thousands of workstations and network connections. To locate the rest of the rogue modems, some manpower will have to be allocated to do modem scanning. However, the terminal server and Windows terminals can be configured not to allow modems. This not only secures a weak link on the network, but the administrator will not have to scan the network for modems.

Applications

All applications run on the server. To keep users from running unapproved software users can be restricted to running only published applications. The Application Security Registration Utility (APPSEC) can be used to limit the applications that non-administrative users can run. Only mouse clicks, desktop images and keystrokes cross the network. This makes it very difficult for a hacker to sniff the wire and get any useful information. In addition, passwords and data that cross the network can be encrypted. For maximum protection, a 128-bit two-way algorithm on both the client and server can be used.

Protecting Shares

With Terminal Services and Windows terminals, data is maintained on the server, and if the Windows NT file system (NTFS) is used, it will provide secure individual and group accounts. The Windows NT file system must be used because it provides access control on files and directories. This allows the administrator to assign access rights by user or groups on a file-by-file basis, and the administrator is assured that the file system is protected according to the security policy.

Malicious Software

Desktop computers can easily be infected by viruses, worms, Trojan horses, and malicious applets via the network, floppy disks and CDROMs. However, Windows terminals without a floppy or CDROM are less likely to be infected. With users' desktops and laptops computers, it is nearly impossible to insure that they are all protected against viruses. When using Windows terminals with no local peripherals, it greatly reduces the chance of introducing viruses. The

greatest risk is with email, but with stringent email filtering techniques, this risk should be significantly reduced. Of course, the servers are still vulnerable especially if they are connected to the Internet. The most recent threat is the Code Red worm, which has infected thousands of computers within minutes that did not have the patch for the Code Red worm installed. With the administrator able to focus on securing the network, they can keep up with the network antivirus software updates, which should eliminate most computer virus problems. The following organizations can help an administrator stay on top of the latest threats and fixes:

- Microsoft
- The National Infrastructure Protection Center
- Federal Computer Incident Response Center (FedCIRC)
- Information Technology Association of America (ITAA)
- CERT Coordination Center
- SANS Institute
- Internet Security Systems
- Internet Security Alliance

Passwords

Password management is the key in a server-based computing environment. With Terminal Server, the administrator can insure the security policy is followed. Most Windows desktop computers store passwords locally in the registry, as well as on the Emergency Repair Disk, and backup tapes. If access is not strictly controlled on these items, the password is at risk of being comprised. There are tools available that allow an attacker to crack a password or change it. This is an awe-inspiring task. How can an administrator possibly insure that the Emergency Repair Disks and backup tapes are secured and physical access to computers is very hard to control as well. However, with Windows terminals, there is no network password stored locally and no need for an Emergency Repair Disk or backup tapes. This eliminates a large burden of an organization concerning how to protect these resources. Windows desktop computers also have the problem of the local administrators password. How much time and effort is required to keep the password secure and change it when an administrator leaves the organization so the password is not compromised. With Windows terminals, the local administrator password is used only for local configuration; if compromised, it would not put data at risk.

Backups

If users have desktops with a local hard disk, is that hard disk backed up? Is it backed up remotely after normal working hours? If so, does the computer have to be powered on? In addition, if the user needs to use the computer when it is being backed up, will it have a detrimental effect on the response of the computer? Will the user reboot during the backup process? If the user backs up locally, is the backup process followed and are data restores

practiced? With Terminal Services and Windows terminals, all backups are done at the server level where it is much better controlled. A written procedure and logs are much easier to control and audit.

Auditing

The greatest risk of attack comes from employees, but by using auditing to monitor file access, habitual patterns can be detected which may indicate improper usage. To insure that your systems are operating optimally and remain secure, auditing has to be done on all the systems. This can be a very expensive proposition in both money and labor. Even if tools are used, which can be expensive, some data will have to be reviewed manually, which is not a small task. With Terminal Services and Windows terminals, all auditing is done at the server level and is a much easier task.

Conclusion

Of course, not all risks can be eliminated, and there is always a price to pay for security. Terminal Services and Windows terminal is not the answer for every situation. However, this model with databases, file servers, and applications in one location is much easier to manage. Business-critical applications and updates can be rolled out instantly across any type of network to any type of client. With the power of single-point control, functions such as deploying, managing, user configurations and security are optimized. Moreover, the user gets access to the most up-to-date applications with the familiarity and ease of use they had with their PC. In some environments, it can be a cost-effective and secure solution.

References

"About Thin Clients, Are there different kinds of thin clients?" URL: http://www.national.com/appinfo/thinclient/thinTypes.html (10 Sep 2001).

"CITRIX, Now everything computes." URL: http://www.citrix.com/ (10 Sep 2001).

Cumberland, Brian, Carius, Gavin, and Muir, Andrew. Microsoft Windows NT Server 4.0 Terminal Server Edition Technical Reference Redmond: Microsoft Press 1999.

Hao, Erica. "Acer WT 300: Busting TCO" 14 July 2001. URL: http://global.acer.com/Products/news.asp?pageID=1409 (10 Sep 2001).

Kaplan, Steve. Maguas, Marc. Citrix MetaFrame for Windows Terminal Services: The Official Guide Berkeley: Osborne/McGraw-Hill, 2000.

Stansel, Paul. Guinn, Travis. Kistler, Kris. Configuring CITRIX METAFRAME for Windows 2000 Terminal Services. Rockland: Syngress Publishing, Inc, 2000.

"Technical Articles - Virus Protection." URL: http://www.pandasecurity.com/tech-articles.htm (10 Sep 2001).

"Thin Planet, For Thin Client and ASP Experts." URL: http://www.thinplanet.com/ (10 Sep 2001).

"Terminal Services Security." Securing a Windows 2000 terminal server. URL: http://www.secadministrator.com/Articles/Index.cfm?ArticleID=16524&Key=Permissions (10 Sep 2001).

"Windows NT Security: Step-by-Step." 5 **Mar. 1998.** URL: http://www.sans.org/newlook/publications/ntstep.htm (10 Sep 2001).

"WYSE." URL: http://www.wyse.com/index_us.htm (10 Sep 2001).

Last Updated: July 25th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event