REMOTE ADMINISTRATION TOOLS: A COMPARATIVE STUDY

Anis Ismail, Mohammad Hajjar, Haissam Hajjar
Department of Computer Network and Telecommunications Engineering
University Institute of Technology – Saida
Lebanese University
Email: anismaiil@yahoo.com, m_hajjar@ul.edu.lb

ABSTRACT

One of the trends we have been observing for some time now is the blurring of divisional lines between different types of malware. Classifying a newly discovered 'creature' as a virus, a worm, a Trojan or a security exploit becomes more difficult and anti-virus researchers spend a significant amount of their time discussing the proper classification of new viruses and Trojans. Depending on the point of view, very often, the same program may be perceived as a Remote Administration Tool (RAT) allowing a potentially malicious user to remotely control the system. A Remote Administration Tool is a remote control software that when installed on a computer it allows a remote computer to take control of it. With remote control software you can work on a remote computer exactly as if you were right there at its keyboard. With fast, reliable, easy-to-use pc from remote control software, it lets you save hours of running up and down stairs between computers. Remote control software allows you to take control of another PC on a LAN, WAN or dial-up connection so you see the remote computer's screen on your monitor and all your mouse movements and keystrokes are directly transferred to the remote machine. Remote control software provides fast secure access to remote PC's on Windows platforms. Hackers and malware sometimes install these types of software on a computer in order to take control of them remotely. Many remote administrator tools exist in the market and it is difficult to choose what you need. As you are an IT support, you need to choose the software which leads your IT skills. After you determine how much you want to manage remotely, the next step is to select the tools and supporting components you need to accomplish your remote management tasks. Our paper entails evaluating many remote control software which help you to select the remote administrator tools.

Keywords— *Remote Administration Tool (RAT), LAN, WAN, control, WMI, RPC, Web.*

1. INTRODUCTION

Companies are looking for ways to provide cost-effective network access to their remote and mobile employees. For chronic problems PCs, applications as remote assistant "remote administrator" can save time by giving you access and control a remote PC via either a network or a dial-up connection. If your friend's or relative's PC is running Windows XP professional, you can access the system remotely for free with a computer running any version of windows, including Windows 95.

Today, providing remote and mobile workers with secure remote access to corporate networks is no longer luxury; it has become a business necessity. Letting employees tap into the office local area network "LAN" from customer sites, hotels, internet cafe and airport kiosks can greatly increase business efficiency, productivity and job satisfaction. But mobile empowerment has a price, measured in IT administration and network security.

As more Information Technology departments centralize and consolidate to reduce cost, many remote sites are left with no on-site IT support. Remote administration of computers is increasingly common because of the significant cost benefits; many tasks can be automated, and the administrator does not have to physically visit each computer [1]. In their whitepaper on Remote

Systems Administration, Stephen Packard and Archie Andrews stated that remote systems administration is a reasonable, economical approach. Also, as networks and servers become critical to nearly all business functions, more IT departments are staffing or providing for some type of round-the-clock monitoring and support. While 7 by 24 support is a great capability, it is limited by the ability to gain physical access to off-site network devices and servers when they lock up or cannot be accessed in-band. Even when the problem occurs during business hours, the lack of on-site IT staff may require an unskilled user to work with the remote IT staff to correct the problem. This is not a good use of the unskilled user's time and may turn a small problem into a large one.

Remote control software provides businesses the ability to login and access computers remotely. Utilizing remote control software enables personnel to transfer files or folders quickly and easily, and communicate by instant message, text chat, or voice intercom from any PC, cell phone, wireless PDA.

This fast, reliable, easy-to-use pc remote control software saves you hours of running up and down stairs between computers. The remote administrator software allows you to take control of another PC on a LAN, WAN or dial-up connection so you see the remote computer's screen on your monitor and all your mouse movements and keystrokes are directly transferred to the remote machine. These softwares provide fast secure access to remote PC's on Windows platforms.

Many remote administrator tools exist in the market and it is difficult to choose what you need. As you are an IT support, you need to choose the software which leads your IT skills. After you determine how much you want to manage remotely, the next step is to select the tools and supporting components you need to accomplish your remote management tasks.

There had been existing comparison charts of many remote administrator softwares that had been done over the Internet. We will mention the important comparison between GoToMyPC and PCAnywhere, and, RemotelyAnywhere and PCAnywhere

Remote-control solutions such as Citrix Online's GoToMyPC and Symantec's PCAnywhere™ are one way to provide cost-effective network access to their remote and mobile employees. With the GoToMyPC Corporate product for enterprises, administrators can roll out and manage a remote access solution in minutes. It is a highly secure and cost-effective way for employees to access their computers and network resources remotely. Employees simply access and work on their computers using any Web browser. This paragraph document demonstrates that GoToMyPC has significant advantages over Symantec's PCAnywhere™ [2].

GoToMyPC is significantly easier to implement, configure and administer than pcAnywhere™. GoToMyPC provides a cost-effective, easy-to-implement, fast and secure way to enable employees to remotely access corporate-network resources. Users find that GoToMyPC is convenient because it works from almost anywhere and requires no configuration.

In contrast to PCAnywhere™, GoToMyPC is a cost-effective solution for providing secure remote access to corporate computing resources without extra staff requirement, loss of security or loss of performance. GoToMyPC is also far more convenient for end users because it does not require any client software, is accessible from any Web browser and does not require prior knowledge of the remote resource.

Administrators can easily deploy a remote-access solution with a minimum of effort. Additional security features can be deployed by administrators to meet existing corporate security policies. Overall, GoToMyPC provides lower total cost of ownership than pcAnywhere™ [2].

If you have settled on Symantec's PCAnywhere for remote access to your corporate network, now is the time to reconsider. RemotelyAnywhere is a more secure, cost-effective, and powerful remote administration solution that provides tools above and beyond just remote control for complete administration of workstations and servers on and off the LAN.

RemotelyAnywhere deploys across your LAN in just minutes, and provides secure remote access to and administration of any machine on which it

is installed. Unlike PCAnywhere, RemotelyAnywhere requires no special client software to be installed on your local machine.

RemotelyAnywhere is packed with robust features such as a dashboard view of system diagnostics, built in FTP and SSH server functionality "in the Server Edition", and superior security and auditing mechanisms for HIPAA, Sarbanes Oxley and other regulatory compliance.

Requiring far less configuration than PCAnywhere, RemotelyAnywhere allows easy and secure access from a Web browser to the remote systems you manage [3].

RemotelyAnywhere provides you with fast and secure remote access to your corporate network. Built from the ground up to seamlessly integrate with and complement existing Windows security structures, it provides easy access to the corporate LAN without enlarging its security perimeter. With its easy maintenance and anytime anywhere technology, RemotelyAnywhere provides a very low total cost of ownership.

The rest of this paper is organized as follows, the different techniques used in remote Administration Tools, are discussed in section two. An Analysis of competitive comparasion between remote administrator tools is discussed in section three, followed by Conclusions and Future Enhancements in section four.

2. DIFFERENT TECHNIQUES USED IN REMOTE ADMINISTRATION TOOLS

The purpose of this section is to present the different methods and tools frequently used to administer remote Windows systems, and which let you able to access a command prompt and perform basic system administration, such as view and/or start/kill processes or services, reboot machines and view system logs, observe what is happening on the display, and even run GUI based programs all remotely, that depends on each features of these remote administrator softwares.

A. MSRPC "Win32 legacy management APIs"

The traditional method to administer remote Windows systems is to use Win32 legacy management APIs. These APIs can be easily identified because they take a server name as one of their parameters, when the server name is empty "NULL", the API operates on the local server, and when a server name is specified, the API operates on the specified remote server. For instance, all APIs with names starting with Net such as NetShareEnum() belong to this class of APIs. When used to administer a remote server, these APIs use the MSRPC protocol, "Microsoft implementation of the DCE RPC standard" with the SMB transport. SMB is the core protocol of Windows networks and operates on both port 139/tcp and 445/tcp. When used as a transport for MSRPC, named pipes inside the IPC$ share are used as RPC services endpoints. [4]

Microsoft Remote Procedure Call "RPC" is an interprocess communication "IPC" mechanism that enables data exchange and invocation of functionality residing in a different process. That process can be on the same computer, on the local area network "LAN", or across the Internet. The Microsoft RPC mechanism uses other IPC mechanisms, such as named pipes, NetBIOS, or Winsock, to establish communications between the client and the server. With RPC, essential program logic and related procedure code can exist on different computers, which is important for distributed applications.

B. WMI "Windows Management Instrumentation"

WMI "Windows Management Instrumentation" is the management framework available in recent Windows systems. WMI is built on the COM "Component Object Model" infrastructure and can thus operate remotely, using DCOM "Distributed COM" [5]. In addition, several WMI-based administration tools are available by default on Windows systems to administer remote systems using WMI.

Windows Management Instrumentation is an infrastructure that enables you to access and modify standards-based information about objects, such as computers, applications, and network components, in your enterprise environment. Using WMI, you can create powerful administration applications to monitor and respond to specific events in your environment. For example, you can create applications to check CPU usage on your Windows Server 2003, based servers and warn you when it exceeds a specified level. Although WMI is a powerful tool for

building customized applications, it does require a certain amount of developing time and expertise.

Windows Management Instrumentation Command-line "WMIC" provides a simplified interface to WMI. By using WMIC, you can access WMI based information using the command line or scripts. You can use WMIC from any computer where WMIC is enabled to manage any remote computer. WMIC does not have to be available on the remote computer.

Currently, testers of the Windows Management Instrumentation "WMI" conduct tests through a proprietary GUI interface, which does not allow for negative testing or the logging of events and methods.

C. GUI-oriented tools build in windows

Many Windows system administrators tend to use graphical remote administration tools that allow access to Windows GUI.

Recent Windows systems "Windows 2000, Windows XP, Windows Server 2003" natively support Terminal Services, the feature of Windows NT that allow multiple concurrent interactive logon sessions. The network protocol used by Terminal Services is RDP, Remote Desktop Protocol, and operates by default on TCP port 3389.

Terminal Services rely on Windows authentication to authenticate users establishing remote sessions. In addition, applicative permissions are supported by Terminal Services to restrict the category of users allowed to establish Terminal Services sessions, Permissions tab in the Properties of the RDP-Tcp transport in Terminal Services Configuration MMC snapin.

Remote Desktop, included with Windows XP Professional, enables you to connect to your computer across the Internet from virtually any computer, Pocket PC, or Smartphone. Once connected, Remote Desktop gives you mouse and keyboard control over your computer while showing you everything that is happening on the screen. With Remote Desktop, you can leave your computer at the office without losing access to your files, applications, and e-mail. Your sales force will be able to access the latest pricing sheet from on the road by using Remote Desktop in Windows XP Professional.

With Remote Desktop, you can connect to your work computer from home and access all of your programs, files, and network resources as though you were actually sitting in front of your computer at work.

D. CLI-oriented tools

CLI "Command Line" remote administration tools are sometimes needed, for instance to execute non-interactively system administration scripts [6].

PsExec is a convenient tool for Windows systems administrators because it allows to execute processes on a remote system, provided the server service is available "TCP ports 445 or 139" and that you have local administrator credentials on the remote system [7].

PsExec first copies its executable, psexesvc.exe, contained in the psexec.exe binary, using SMB, under %systemroot%\System32\, installs the service and starts it. These steps require administrator credentials.

If you are logged on with local credentials that also correspond to local administrator credentials, with a domain administrator account or with an account with username and password identical to a local administrator account on the remote system, additional credentials are not needed.

Rcmd is a Windows NT 4.0 Resource Kit tool composed of a Windows service and a command-line client that supports remote process execution. The Rcmd service opens a named pipe, \pipe\rcmdsvc. The Rcmd client establishes an SMB session to the IPC$ share, authenticated with an account that needs to have the SeInteractiveLogonRight logon right "Allow log on locally".

E. Web based tools

One of the major issues confronting information systems "IS" managers today is how to provide secure access to corporate IS resources to people who are physically located outside of the corporate network. In today's increasingly connected society, traveling salespeople, telecommuters and staff working extra hours all need real-time access to resources on corporate networks.

For security reasons, these resources, such as databases, sales tools and email are usually protected by firewalls so that users outside the

corporation cannot access them. Companies are looking for ways to provide cost-effective network access to their remote and mobile employees. Many Remote-control solutions are one way to provide this access.

The Web based remote administration tools like GoToMyPC is a hosted service that enables secure browser-based access to any Internet-connected Microsoft Windows-based PC. Features include a screen-sharing Viewer, drag-and-drop File Transfer, Remote Printing, Guest Invite and Chat. Corporate administrators have access to extensive management and reporting tools that enable central control over these remote-access services.

While choosing a Windows remote administration tool, the following characteristics have to be considered the TCP ports required to use the remote administration feature the supported authentication mechanisms, system authentication implemented by Windows, application level authentication only.

3. COMPARISON AND ANALYSIS

In this paragraph, we mention the availability of features in each remote administrator tools. In addition of chart on each group of features, it will present the strengths of these remote administrator tools. These charts help the IT to choose the remote administrator tool that leads their professional skills.

We did this experiment for a couple of reasons. First, it seemed like a great academic exercise. There's a certain challenge that comes from administering your organization's web server or Primary Domain Controller via a small handheld computer. However, there's also the allure of being truly able to administer servers remotely without having to carry around a laptop.

The advantage of such a model, should it prove successful, is an ability to carry a pocket-sized device and yet have full remote terminal capabilities. You'd not have to leave other situations for some emergencies. Instead use your handheld device to solve the problem over a phone line, Ethernet, or wireless link. The usefulness of this becomes very apparent when you're at some social event or in a meeting.

F. Features

Figure 1 represents the availability of these features "Main Features" in the available products in the market. These features are Support Different Resolutions, Support Different Color Depth, Remote Clipboard, Simultaneous Multi-Protocol, Simultaneous Control & Client, Multiple Controls, View Multiple Clients, Printer Redirection, Scaleable Windows Record & Replay Session, Watch, share, Control a Client PC, Send Ctl-Alt-Del, Remote Reboot, Blank Client Screen and Web Browser Integration.

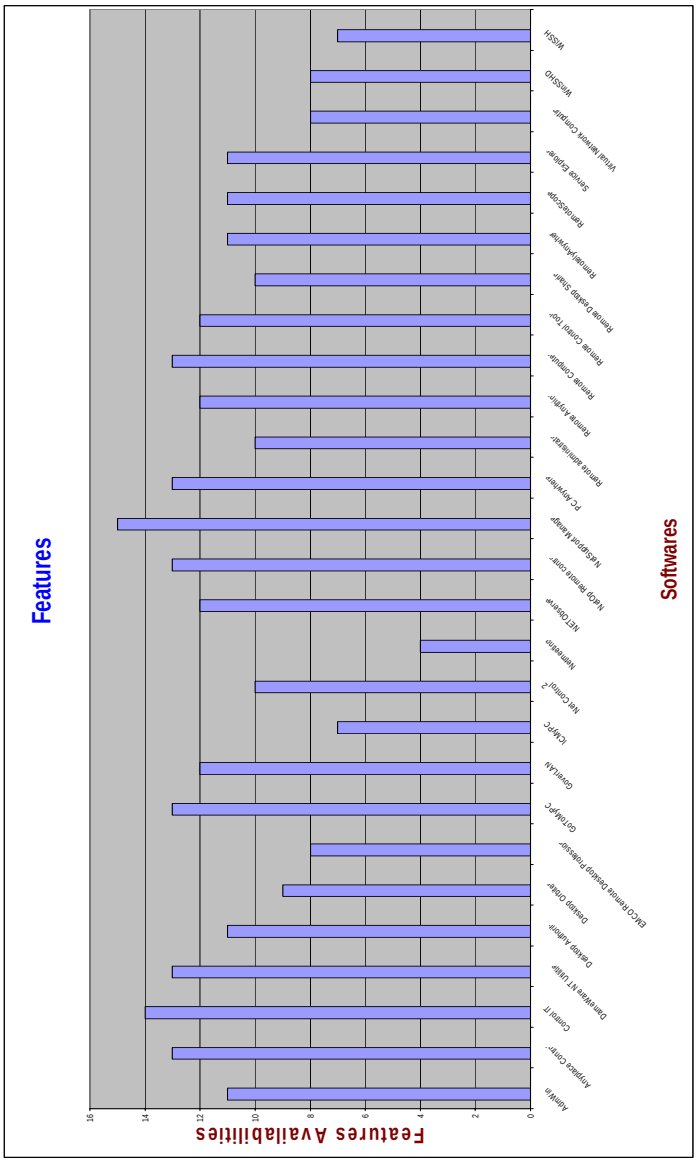


Figure 1 - Main features

G. File Transfer

Figure 2 represents the availability of these features "File Transfer" in the available products mentioned in the market. These features are One to One File Transfer, Synchronize Drives and Directories, Support long file names, File Compression and Launch Remote Applications.

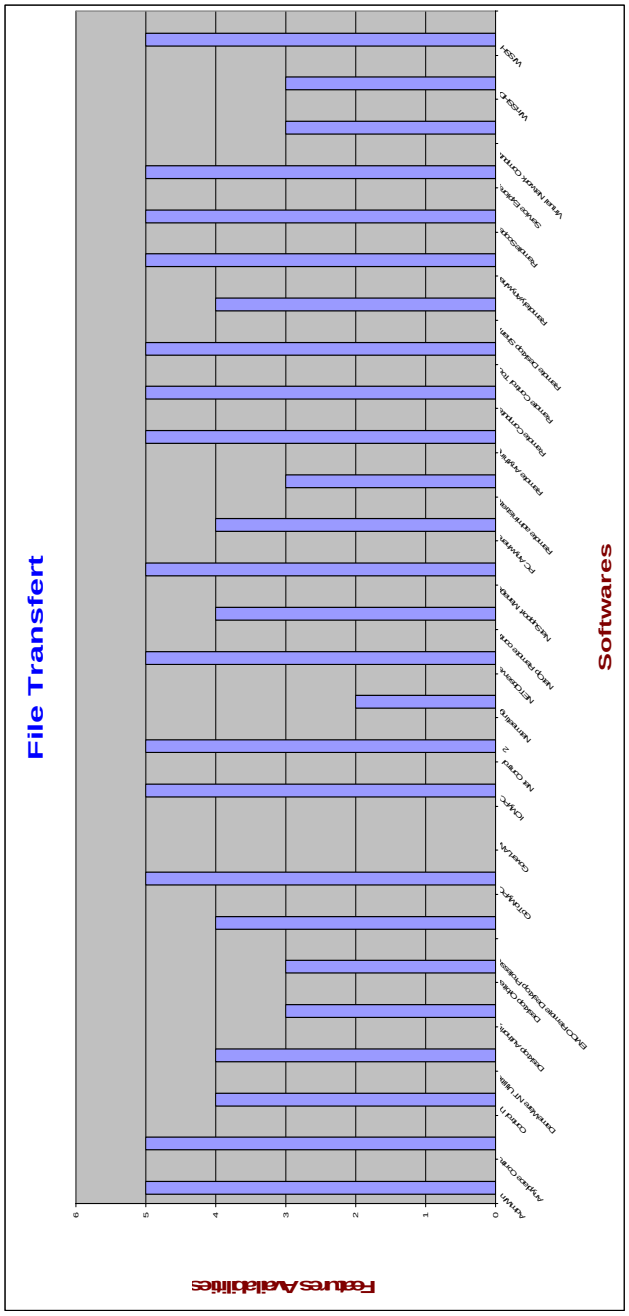


Figure 2 - File Transfer Features

H. Misc Feature

Figure 3 represents the availability of these features "Misc Features" in the available products mentioned in the market. These features are Telnet, Remote Deployment of Software, Group Connect at Startup, View Multiple Clients Simultaneously, Chat, Scripting and Silent Installation.

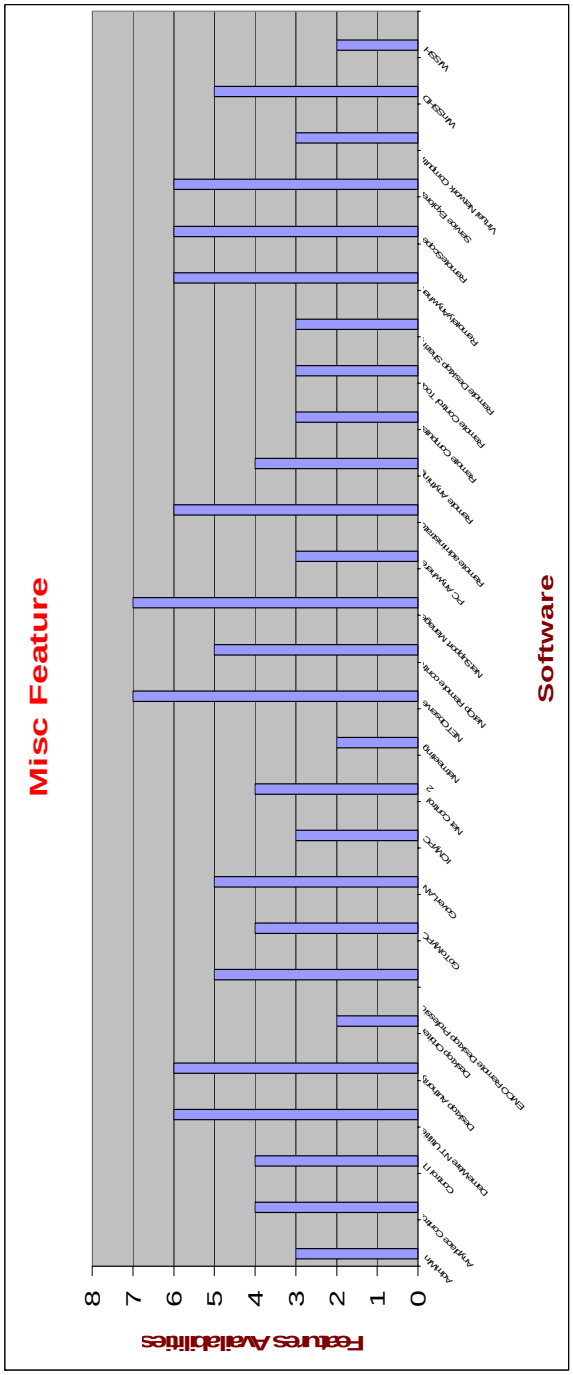
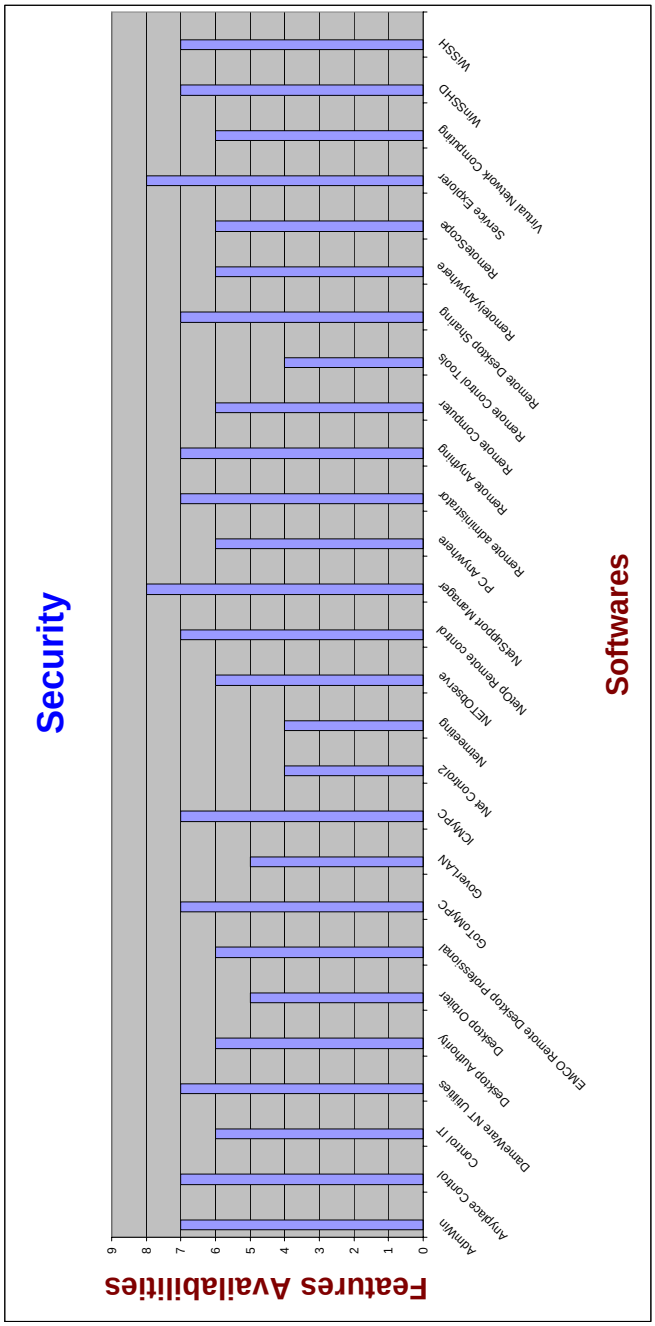


Figure 3 - Misc Features

Figure 4 - Security Features

I. Security

Figure 4 represents the availability of these features "Security" in the available products mentioned in the market. These features are Password Encryption, Dial Back, Use Windows 2000 Profiles, User Acknowledgement at Client, Password Protection at Client/Control, DES Encryption, Use NT Profiles, and Audit Log.



J. Protocol Support

The Figure 5 represents the availability of these features "Protocol Support" in the available products mentioned in the market. These features are IPX/SPX, NetBIOS, TCP/IP and NetBEUI.

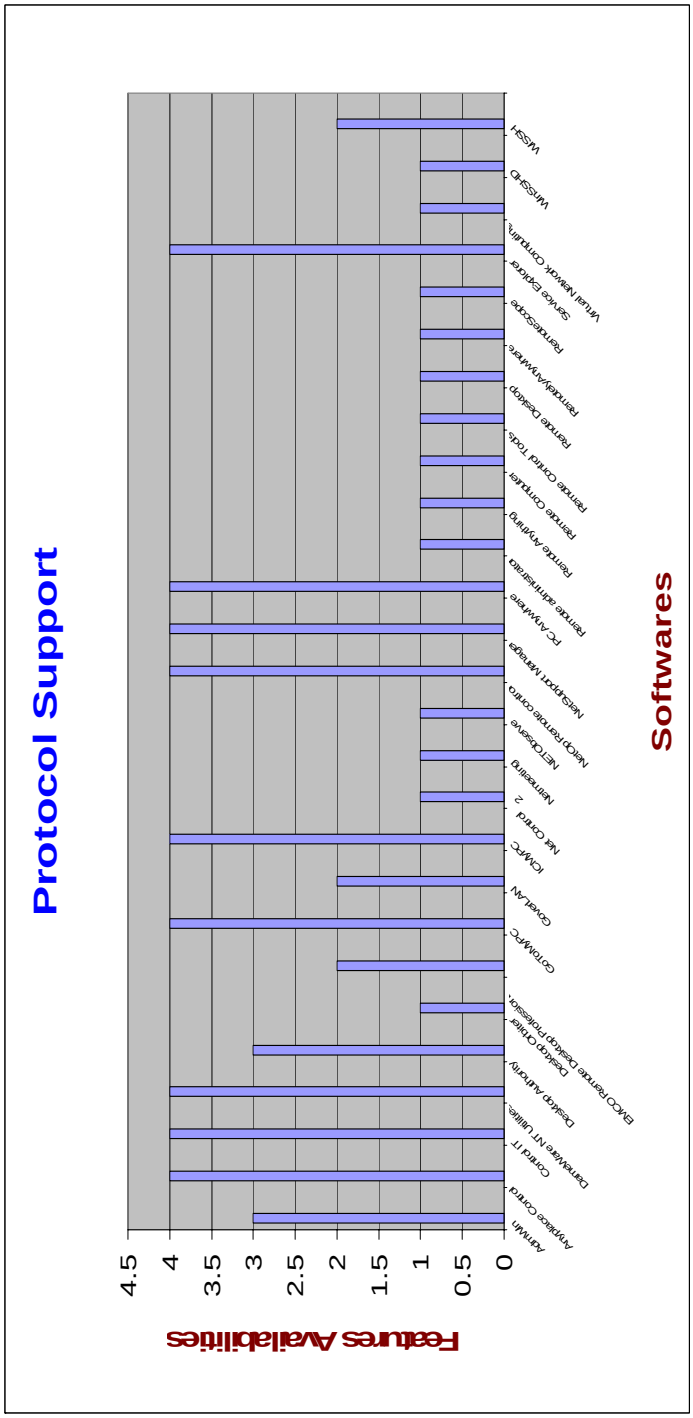


Figure 5 - Protocol Support

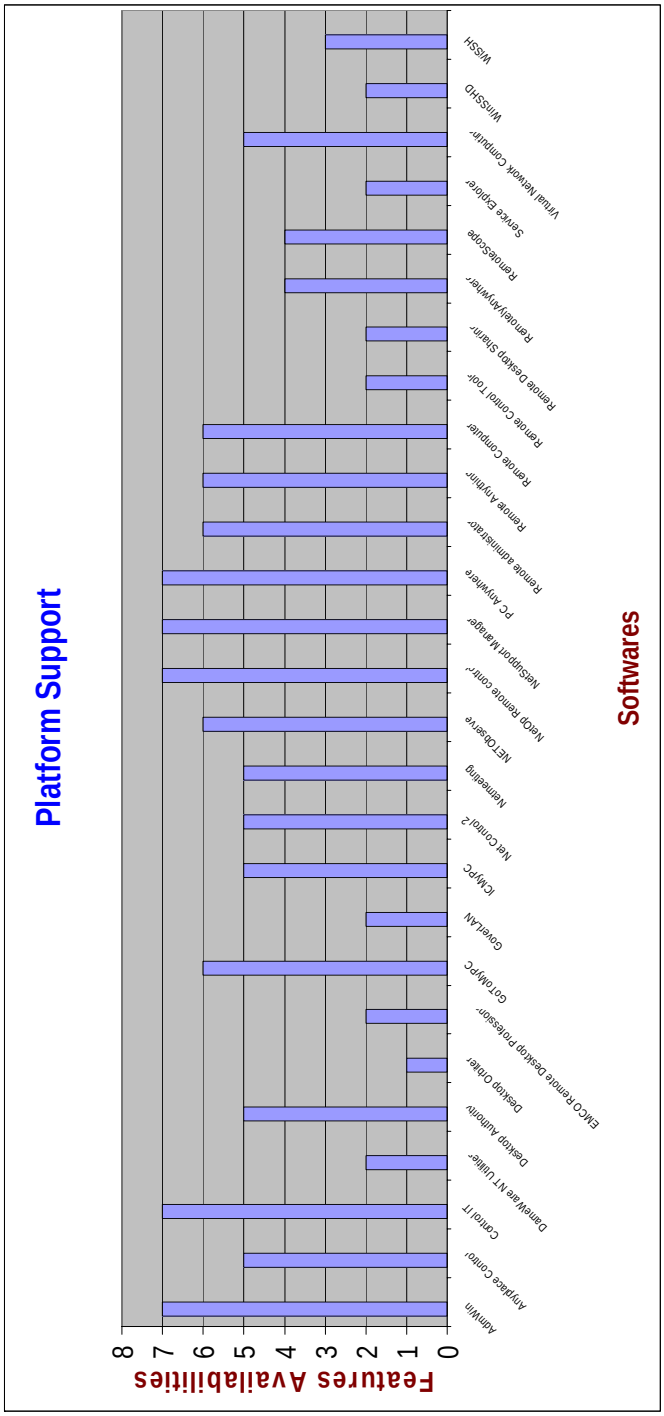
Figure 6 - PlatForm Support

K. Platform Support

The Figure 6 represents the availability of these features “Platform Support” in the available products mentioned in the market. These features are Windows 95, Windows 98, Windows "ME", Windows 2000/XP, NT 3.X, NT 4.00, Linux.

L. Connectivity

Figure 7 represents the availability of these features “Connectivity” in the available products mentioned in the market. These features are Analogue Modem, ISDN, WAN, LAN and Wireless IRDA.



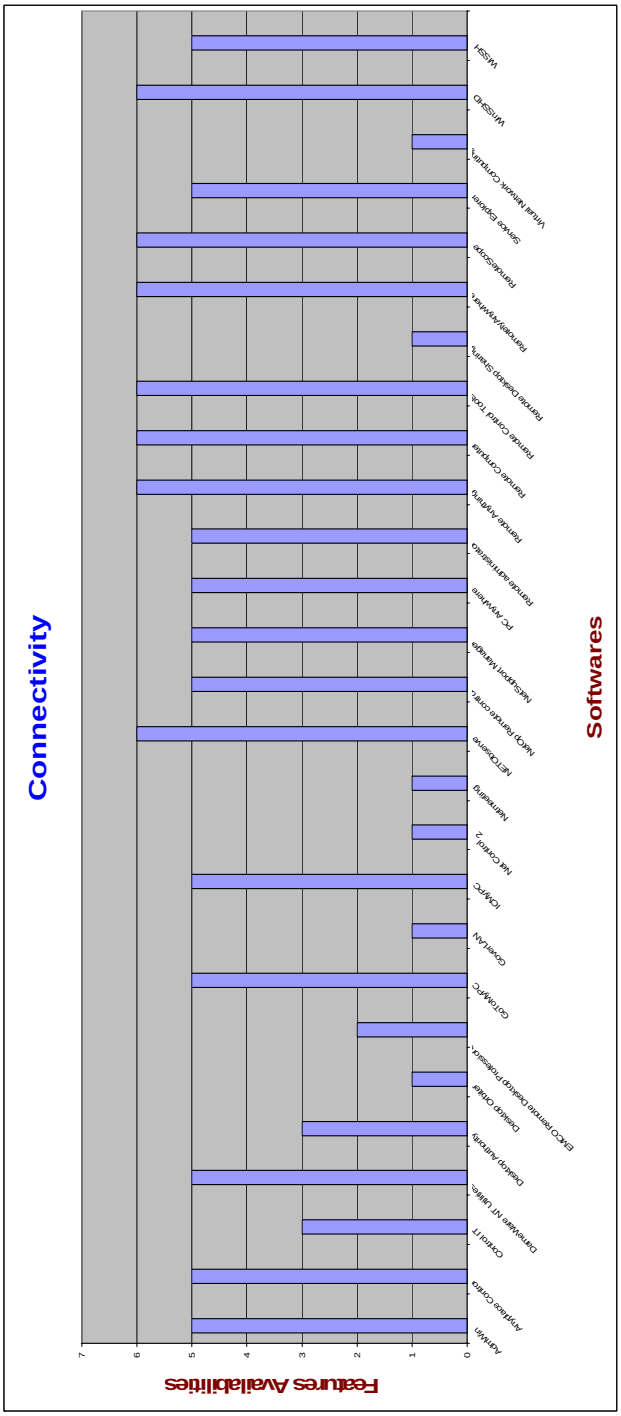


Figure 7 - Connectivity Support

4. CONCLUSION

Using remote administrator tools for graphical remote administration of computers running Windows can greatly reduce the administrative overhead in any Windows 2000 Server or windows workstation environment. Administrators can access the servers from anywhere, be it inside the computer room or from halfway around the world over a WAN, VPN, or dial-up connection. They can start time-consuming batch administrative jobs (for example, tape backups), disconnect, and dial-in to the corporate network at a later time to check the progress.

Server application and operating system upgrades can be completed remotely, as well tasks that are not usually possible unless the administrator is sitting at the console, such as domain controller promotion/demotion and disk defragmentation. Server file system tasks such as copying large files and virus scanning are much more efficient when performed within a remote tools session, rather than using utilities that are executed on a PC client.

Administration tasks are quicker and more intuitive than using command line utilities, although it is still possible to open up a command shell. Administrators can also fully administer Windows 2000 Servers using non-Windows 2000 clients.

Remote administrator tool is an affordable tool that any small business owner can purchase without having to consult his accountant. Companies offer very flexible licensing policies for Remote administrator tool that cover multiple computers at minimal expense.

Remote administrator tool has no special hardware requirements. Even if your old home computer is what you use for running your business, it’s fast enough for Remote administrator tool. If the computer runs Windows, Remote administrator tool will run on it, and it will run faster than any other remote control software you can buy.

An evaluation is being built on existing remote administrator tools of the availability of features and is expected to be one of the important evaluations used by major high-energy research. This evaluation let customers choose their need of remote administrator tools carefully.

REFERENCES

[1] CERT, Configure computers for secure remote administration, 2000, URL: http://www.cert.org/security-improvement/practices/p073.html.

[2] 1997-2004 Citrix Online, a division of Citrix Systems, Inc. All, Citrix Online Division 5385 Hollister Avenue Santa Barbara, CA 93111, 1997-2006. URL: https://www.gotomypc.com /ourTechnology.tmpl? SessionInfo=12759838:5F8BC3C78C05104

[3] RemotelyAnywhere™ and pcAnywhere™: a Comparison 3am Labs, 2005. URL: http://www.remotelyanywhere.com/RA_vs_pc Anywhere _v6.pdf

[4] Hervé Schauer Consultants, Jean-Baptiste Marchand, Windows network services internals, 2003, 2004, 2005, 2006. URL: http://www.hsc.fr/ressources/articles/win_net_srv/

[5] Microsoft Technet's Script Center, 2006. URL: http://www.microsoft.com/technet/scriptcenter/

[6] Mark Russinovich, The PsExec utility, part of Sysinternal's PsTools, 1999-2006. URL: http://www.sysinternals.com/ntw2k/freeware/pstools.shtml.

[7] Mark Russinovich, PsExec supports several options, 1999-2006. URL: http://www.sysinternals.com/ntw2k/freeware/psexec.shtml