Global Information Assurance Certification Paper

Securing Remote Control Software for safe IT-Support

Patrick Heinen
April 16, 2003

Introduction

Remote control software is often used as a powerful tool for delivering higher quality support to PC users and containing rising support costs. Remote control tools allow support technicians to assume control of a user's PC or an unattended server - over the network and dialup connections - and work with it as if it were local. This enables support staff to resolve problems quickly and easily - without ever leaving their desk, no matter how far from the user they are located.
Many companies, however, hesitate to take advantage of these compelling savings because of security concerns. Remote access could expose PCs and the corporate network to intrusion from outside the enterprise.
This paper examines the security issues that companies should consider when implementing remote control software for remote support. It also defines the requirements for a remote control solution that addresses enterprise security needs. There also is a comparison between an Operation System build in Remote Control Software like in Windows 2000 Server and Windows XP, and a Third Party Product like Symantec pcAnywhere.

Security concerns

The increasing complexity of PC software, hardware and networks, combined with the growing number of users accessing the network from remote locations, complicates the requirements of a cost efficiency support centre. The financial benefits of remote control software as a support tool, can be significant and allows to lower annual support costs by 6 to 13 percent. IT Professionals have to troubleshoot hundreds of users and resolve support problems just in time. This all should be done without raise travel expenses so the only way to build up a cost efficiency support centre is to use remote control software. Although Remote control software is a powerful software for helpdesk support it raises security issues and the ability of being attacked.
Without proper security, remote access to a PC (a host) could potentially expose the PC to access by an unauthorized user. The intruder might obtain confidential information stored on that PC, sensitive corporate information such as trade secrets and employee data. Furthermore, the intruder might be able to tap into all network resources that are available to that PC without been identified. Using insecure remote control software on unattended servers raises the ability that a hacker could change user rights and maybe adds new users with administrative rights.
Applying security is extremely difficult with dial-in or Internet connections in which users access the network from outside the corporate network. But even for users located inside a corporate network, unauthorized access is often a big problem. Their desktops should not been able to be taken over without the administrative rights for it.
Another problem is the ability to copy data without the knowledge of the person sitting in front of the PC that the helpdesk is connected to. Some remote control products allow to copy data to and from the PC in the background. A secure product should be able to block this for specific folders which the helpdesk should not look at.

Newest operation systems like Windows 2000, 2003 Server and Windows XP allow remotely connecting to the desktop without a special product. The Windows 2000 and 2003 Servers have a Terminal Server option which can be used for remote administration also. This build in functionality allows building up a companywide remote control solution very easily. The problem is that there is no build in security. System Administrators have the ability to connect to a users PC or a server without authorisation. The standard system has no encryption so there is a possibility that somebody accesses the remote connection without the administrator's knowledge. Furthermore there are some known vulnerabilities in the build in remote control system from Microsoft:

This Information is from www.securityfocus.com/bid/5713

Microsoft Windows XP Professional Remote Desktop Denial Of Service Vulnerability

Information:

bugtraq id	5713
object	
class	Failure to Handle Exceptional Conditions
cve	CAN-2002-0864
remote	Yes
local	No
published	Sep 16, 2002
updated	Sep 19, 2002
vulnerable	Microsoft Windows .NET Standard Server Beta 3 Microsoft Windows 2000 Advanced Server SP3 Microsoft Windows 2000 Advanced Server SP2 Microsoft Windows 2000 Advanced Server SP1 Microsoft Windows 2000 Advanced Server Microsoft Windows 2000 Datacenter Server SP3 Microsoft Windows 2000 Datacenter Server SP2 Microsoft Windows 2000 Datacenter Server SP1 Microsoft Windows 2000 Datacenter Server Microsoft Windows 2000 Professional SP3 Microsoft Windows 2000 Professional SP2 Microsoft Windows 2000 Professional SP1 Microsoft Windows 2000 Professional Microsoft Windows 2000 Server SP3 Microsoft Windows 2000 Server SP2 Microsoft Windows 2000 Server SP1 Microsoft Windows 2000 Server Microsoft Windows 2000 Terminal Services SP3 Microsoft Windows 2000 Terminal Services SP2 Microsoft Windows 2000 Terminal Services SP1

	Microsoft Windows 2000 Terminal Services
	Microsoft Windows XP 64-bit Edition
	Microsoft Windows XP Home
	Microsoft Windows XP Professional
not vulnerable	Microsoft Windows XP 64-bit Edition SP1
	Microsoft Windows XP Home SP1
	Microsoft Windows XP Professional SP1

Discussion:

The Microsoft Windows XP Professional Remote Desktop implementation is prone to a denial of service.

It is possible for a malicious client to trigger this condition by sending a maliciously crafted packet to the vulnerable host during the negotiation of client/server graphics capabilities. Clients may specify drawing commands based on what is supported. If the Pattern BLT command is specified in a packet, Microsoft Windows XP Professional will crash when it tries to render the pattern.

This issue also exists in Microsoft Windows .NET Standard Server Beta 3.

Exploit:
The following exploit information was provided:

Shown below is the unencrypted packet contents for the problematic PDU Confirm Active packet. The only change is from 01 to 00 on the line indicated.

```
c4 01 13 00 f0 03 ea 03 01 00 ea 03 06 00 ae 01
4d 53 54 53 43 00 11 00 00 00 01 00 18 00 01 00
03 00 00 02 00 00 00 00 05 04 00 00 00 00 00 00
00 00 02 00 1c 00 08 00 01 00 01 00 01 00 00 05
00 04 00 00 01 00  01 00 00 00 01 00 00 00 03 00
58 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 01 00 14 00 00 00 01 00 00 00
2a 00 01 00 01 01 01 00 00 01 01 01 00 01 00 00 <  - was "2a 00 01 01"
00 01 01 01 01 01 01 01 01 00 01 01 01 00 00 00
00 00 a1 06 00 00 00 00 00 00 00 84 03 00 00 00
00 00 e4 04 00 00 13 00 28 00 01 00 00 03 78 00
00 00 78 00 00 00 f3 09 00 80 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00
08 00 06 00 00 00 07 00 0c 00 00 00 00 00 00 00
00 00 05 00 0c 00 0 0 00 00 00 02 00 02 00 08 00
0a 00 01 00 14 00 15 00 09 00 08 00 00 00 00 00
0d 00 58 00 05 00 08 00 09 08 00 00 04 00 00 00
00 00 00 00 0c 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00  00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 0c 00 08 00 01 00 00 00
0e 00 08 00 01 00 00 00 10 00 34 00 fe 00 04 00
```

fe 00 04 00 fe 00 08 00 fe 00 08 00 fe 00 10 00
fe 00 20 00 fe 00 40 00 fe 00 80 00 fe 00 00 01
40 00 00 08 00 01 00 01 03 00 00 00 0f 00 08 00
01 00 00 00 11 00 0c 00 01 00 00 00 00 0a 64 00
14 00 08 00 01 00 00 00 15 00 0c 00 01 00 00 00
00 0a 00 01

Solution:

Workaround:
It is possible to disable the Remote Desktop. This will eliminate exposure to this vulnerability.

Solution:
Microsoft has released patches:

Microsoft Windows 2000 Professional SP3:
Microsoft Patch Q324380
http://www.microsoft.co m/Downloads/Release.asp?ReleaseID=41326

This patch addresses RDP 5.0 included with Windows 2000.

Microsoft Windows 2000 Server SP3:
Microsoft Patch Q324380
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=41326

This patch addresses RDP 5.0 included with Windows 2000.

Microsoft Windows 2000 Advanced Server SP3:
Microsoft Patch Q324380
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=41326

This patch addresses RDP 5.0 included with Windows 2000.

Microsoft Windows 2000 Terminal Services SP3:
Microsoft Patch Q324380
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=41326

This patch addresses RDP 5.0 included with Windows 2000.

Microsoft Windows 2000 Datacenter Server SP3:
Microsoft Patch Q324380
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=41326

This patch addresses RDP 5.0 included with Windows 2000.

Microsoft Windows 2000 Advanced Server SP2:
Microsoft Patch Q32438 0
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=41326

This patch addresses RDP 5.0 included with Windows 2000.

Microsoft Windows 2000 Datacenter Server S P2:
Microsoft Patch Q324380
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=41326

This patch addresses RDP 5.0 included with Windows 2000.

Microsoft Window s 2000 Professional SP2:
Microsoft Patch Q324380
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=41326

This patch addresses RDP 5.0 included with Windows 2 000.

Microsoft Windows 2000 Server SP2:
Microsoft Patch Q324380
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=41326

This patch addresses RDP 5.0 included with Windows 2000.

Microsoft Windows 2000 Terminal Services SP2:
Microsoft Patch Q324380
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=41326

This patch addresses RDP 5.0 included with Windows 2000.

Microsoft Windows XP 64 -bit Edition :
Microsoft Patch Q324380
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=4 1314

This patch addresses RDP 5.1 included with Windows XP 64 bit Edition.

Microsoft Windows XP Professional :
Microsoft Patch Q324380
http://www.microsoft.com/Down loads/Release.asp?ReleaseID=41288

This patch addresses RDP 5.1 included with Windows XP Home/Professional.

Microsoft Windows XP Home :
Microsoft Patch Q324380
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=41288

This patch addresses RDP 5.1 included with Windows XP Home/Professional.

Credit:
Discovery of this issue is credited to Ben Cohen and Pete Chown of Skygate Technology Ltd.

There are other known vulnerabilities too, and Microsoft has fixed them already but the risk is that somebody uses this system without the knowledge of the risks. When you want to encrypt the RDP session, which should be done whenever communicating over the internet, you have to make some adjustments in the build in system, too.

This article is taken from the Microsoft TechNet website:

HOW TO: Use IPSec Policy to Secure Terminal Services Communications in Windows 2000

The information in this article applies to:
Microsoft Windows 2000 Server
Microsoft Windows 2000 Advanced Server
Microsoft Windows 2000 Datacenter Server

SUMMARY
You can use Windows 2000 Terminal Services to gain access to programs in a multiple-user Terminal server environment. Communications between the Terminal Services client computer and the server that has Terminal Services enabled can contain sensitive information; therefore, you may want to optimize security between the Terminal Services client and the Terminal server. This step-by-step article describes how to configure the Terminal server to require varying degrees of encryption by using the RC4 algorithm to secure Terminal Services communications.

Many organizations use standardized Internet Protocol security (IPSec) for network security. You can configure IPSec policies on Terminal servers to force all Terminal Services communications to be protected by IPSec.

This article assumes that you are configuring computers that are a part of a domain structure. If the computer is not part of a domain structure, you may also have to configure encryption and authentication services.

For additional information about troubleshooting IPSec, click the article number below to view the article in the Microsoft Knowledge Base:
257225 Basic IPSec Troubleshooting in Windows 2000
To enable IPSec protection for Terminal Services:
Create an IPSec filter list to match Terminal Services packets.
Create an IPSec policy to enforce IPSec protection, and then enable the policy.
Enable the Client (respond-only) policy on the Terminal Services clients.
back to the top
How to Create the IPSec Filter List for Terminal Services Communications
Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Local Security Policy**.
Click to expand **Security Settings**, right-click **IP Security Policies**, and then click **Manage IP filter lists and filter actions**.
Click the **Manage IP Filter Lists** tab, and then click **Add**.
Type **terminal services** in the **Name** box, and then type **for terminal services connections** in the **Description** box.
Click to clear the **Use Add Wizard** check box, and then click **Add** .
Click the **Addressing** tab, click **My IP Address** in the **Source address** box, and then click **Any IP Address** in the **Destination address** box.

After you complete this step, the filter is applied to outbound packets.
Verify that the **Mirrored** check box is selected.

If this check box is selected, a packet filter is created to match inbound packets. All IPSec-secured communications must be protected in both directions; you cannot have unidirectional IPSec security.
Click the **Protocol** tab, click **TCP** in the **Select a protocol type** box, and then click **From this port**
Type **3389** in the **From this port** box, click **To any port**, and then click **OK**.
Click **Close**, and then click **Close**.
back to the top
How to Create and Enable IPSec Policy to Secure Terminal Services Communications
Start the Local Security Settings Microsoft Management Console (MMC), right-click **IP Security Policies** in the left pane, and then click **Create IP Security Policy**.
After the IP Security Policy Wizard starts, click **Next**.
On the **IP Security Policy Name** page, type **secure terminal services connection** in the **Name** box, and then click **Next**.
Click to clear the **Activate the default response rule** check box, and then click **Next**.
On the **Completing the IP Security Policy Wizard** page, verify that the **Edit properties** check box is selected, and then click **Finish**.
Click the **Rules** tab, click to clear the **Use Add Wizard** check box, and then click **Add**.
Click the **IP Filter List** tab, and then click **Terminal Services IP Filter List**.
Click the **Filter Action** tab, and then click **Require Security**.
Click **Apply**, and then click **OK**.
Verify that the **Terminal Services Filter List** check box is selected, and then click **Close**.
Right-click the new policy, and then click **Assign**.
back to the top
How to Ensure That Clients Respond to the Terminal Server's Requests for Security
Click **Start**, point to **Programs**, point to the **Administrative Tools**, and then click **Local Security Policy**.
Click to expand **Security Settings** in the left pane, right-click the **Client (respond only)** policy, and then click **Assign**.
back to the top
Troubleshooting
To verify that IPSec is working, use the IPSec Monitor utility.

For additional information about IPSec Monitor, click the article number below to view the article in the Microsoft Knowledge Base:

Another vulnerability is the Instant Messaging (IM) system which should be used to get in contact with the support technician. Instant Messaging systems are normally used as a simple chatting service. Today's Instant Messaging services allow more features than the simple chatting with another person over the internet. Having more features like file transfer, taking over somebody's desktop with the RDP service means more abilities of being hacked. Instant Messaging systems use simple peer to peer communication without any encryption. There are some known vulnerabilities and exploits:

Account hijacking
Somebody is able to spoof a users account and impersonate that user in conversations with others.

Password Protection
The password protection in IM Systems is often very limited. You do not have minimum password requirements and no strong passwords. Often the passwords are stored plain in the IM system. There are several detailed instructions available that describe how to crack passwords in IM systems.

Modifications in IM Systems
IM Systems do not have an integrity check of the software. Hackers might be able to send buffer overflows or malformed data packets using a vulnerability in the IM system to gain access to the PC.

Worms and Blended Threats
IM Systems could be used for spreading worms and blended threats (as code red). Like email systems using contact groups IM systems use buddy lists to interact with other people easily. These buddy lists could be used by worms to spread itself over the IM system. There are several known exploits for some IM systems.

Denial-of-Service
IM Systems are susceptible to denial-of-service attacks. Am Attacker could send large numbers of specially crafted TCP/IP packets to IM servers to shut the service down. In this case the system can not be used until the provider has fixed the problem.

Instant messaging server vulnerabilities
All vulnerabilities which are described above are client vulnerabilities. But all these vulnerabilities are potentially IM server vulnerabilities, too.

If you have patched the Microsoft system like shown before, you have a more secure system than the original one. But there are more security requirements for a company wide remote control solution which you definitely can't build up with the Microsoft system.

Security requirements

Remote control software using today, has to support various types of security features to meet today's demanding security requirements. Remote control software should support the existing network security infrastructure, including both network- and desktop- based security. The trust and the confidence of the users being supported by a remote control solution is very important for today's companies. The company must feel secure that the corporate network is protected from access via PCs enabled for remote control. Overall, the remote control solution should provide security features that address two major areas:

- Prevention of unauthorized access through strong authorization and access-control mechanisms.
- Monitoring remote connection activities on each host PC through audit trails and activity logs.

(1) Authorization and access control

The remote control software should have a variety of features that protect host PCs against access without the user's knowledge or permission. Examples include:

- Password protection to prevent unauthorized access to the PC. A further restriction would specify who is authorized to start remote control sessions on a particular host.
- Callback capabilities to confirm the caller identification
- Encryption to keep eavesdroppers from listening in on remote connections.
- Restrictions on drive access and file transfer rights.
- Host connect acknowledgments to allow a PC user to confirm or deny access.
- Access by specific remote control systems only. This may include serialization of all hosts and remote control workstations, allowing connection only between host and remote control PCs that have matching serial numbers.
- Restrict access from outside your organisation to internal machines. This may include the limitation of connections to a specific TCP/IP address range.

(2) Authentication

No authentication technique is foolproof, but there are some minimum requirements for a remote control solution. It takes the users credentials and verifies them against a directory service or a access list to determine if the user is authorized to connect the system. Multiple authentication methods like Active Directory Service (ADS), Novell Directory Service (NDS), Lightweight Directory Access Protocol (LDAP) as well as a mandatory operating system authentication like NT authentication (NTLM), Kerberos or secure shell (SSH) should be included as a standard for every remote control solution.

(3) Device control

There are some features which should be provided by the software to protect critical information during remote control sessions.

- Screen and keyboard locking when the PC is idle, making it safe to leave the PC unattended while waiting for remote access.
- Host screen disable to ensure privacy during remote control sessions in which the user is not present.
- The ability to disallow telephone connection to ensure that remote control sessions occur only through a direct network connection and not through dial-in. This allows remote access through either a remote access server or VPN (Virtual Private Network) connection.

(4) Disconnection handling

The host PC should always be protected by the security system after disconnection to ensure that ending a remote control session - either normally or through an unexpected loss of connection - does not leave the host vulnerable to intrusion. It should run as a service in order to support a reconnect after an abnormal reboot of the server or client.
It should also provide a means for handling abnormal disconnections. When a connection is lost unexpectedly, the host should enter a waiting state that allows reconnection, but only by the caller who was disconnected or by a caller with administrative rights.

(5) Configuration control

The IT staff should be able to secure the remote control client software. This prevents users from inadvertently exposing their systems to unauthorized access by changing security settings. It also prevents unauthorized users from reconfiguring the software for their own purposes.
Integrity checking features verify that the software components (like DLL files, executables and registry settings) have not been changed since the initial installation. There also should be an option of serialization of Remote Control hosts. This option allows administrators to put a specific serial number in every host, which only administrators with this serial number listed in their remote control software can connect to. This prevents administrator with the knowledge of username and password for the host to connect unauthorized.

(6) Secure Internet access

The software should enable secure remote control sessions over the Internet - all the way from the host to the helpdesk. This requires support for encryption, for example, symmetric or public key encryption. Encryption prevents the data stream (including the authorization process) from being viewed.
In addition, because of the growing popularity of access through the Internet, the software should support VPN technology to permit secure connections over the Internet through a firewall, as well as over a corporate intranet.

(7) Centralized security management

Security should be supported companywide so the system should be able to support the network-based and the desktop-based part. This allows system administrators a very simple security management over the whole company infrastructure. It also reduces the costs of managing the remote controls solution. The simpler the software is to use the lower is the risk of incorrectly configured security systems. If your security management integrates in your existing environment the easier and the more cost efficiency it is to use. This could be a connection to the NT User Database or Active Directory for authentication with existing users. If an administrator leaves the company other administrators are able to deactivate his account in just one application. This is easier and safer than managing it in different applications because people can't forget applications which the administrator already could have

access to. This also reduces costs of administration because you only have to manage one database.
It is also often a requirement for enterprise customers that a remote control software has got the ability to interact or integrate in existing enterprise management solutions like Microsoft SMS, Tivoli TME or TNG Unicenter from Computer Associates. An interaction between these systems allows better security for example by using SNMP traps or monitoring log files with these existing systems. There is no need to build up second alerting system because of the communication with the existing one. Some enterprise management solutions have remote control solutions but they don't meet the security requirements.

(8) Alerting, logging and reporting

Alerting, logging, and reporting are essential to help maintain a secure environment. The remote control solution should have a centralized logging and reporting in which all log files of the clients and servers come together. The log file should no only log the connection time and name of the connection user, but also what the user has done. When different system administrator connect to a server it is very important that every user reports what he has changed on the server or client. If the remote control solution tracks this in the log file too, to ability to change something on a server or client without writing down what has changed is completely impossible. An audit of the log file can alert disallowed connections to specific server or clients. In addition, the host should issue an alert whenever anyone attempts to start a remote control session on a host and security is not enabled on that host. This ensures that the host is protected even if the user has failed to set up password protection or other security.

(9) Policy considerations

The remote control solution should be able to meet the requirements of secure administration of networks, servers and workstations. Companies which are supported by third parties like contractors, service providers or other vendors should have a special security policy in which the rights of the third parties is defined. CERT recommends a three-step approach for contracted IT services: Preparing, Managing and Concluding.

Rich set of security features

The following table provides numerous security features. This table can be used as a checklist for evaluation purposes:

Feature	**Description**
Full operating system integration	Runs – for example - as an NT service.
Password protection	Protects against unauthorized access

Host security alert	Issues an alert on the host when anyone attempts to start a remote control session on that host and security is not enabled.
Multi-level data encryption	Protects against data theft.
Lock Host PC	Makes it save to leave the PC unattended and enabled for a further remote control session.
Host screen disable	Ensures privacy during remote connections.
Remote keyboard / mouse disable	Increases control over data input and access.
Host connect acknowledgment	Allows a user to allow or deny access to the host PC
Caller list	Specifies people who are authorized to access the host remotely and prohibits others from starting a remote session.
Callback telephone number	Confirms the caller by returning the call to a specified telephone number.
File transfer rights	Restricts file transfer activities to none, upload/download only or full transfer rights.
Drive security	Restricts remote users from accessing specified drives.
Log failed connections	Helps detect attempted security violations.
Limit time online	Ensures resources on the host PC are not monopolized and are available to all users.
Reboot on disconnect	Ensures that the host does not remain in a waiting state after disconnection from another remote session.
Unique “locked” host and remote	Restricts access, allowing the locked host to be accessed only by the corresponding locked remote.
Serialization	Remote PC’s can connect only to hosts that have matching serial numbers.
Central Logging	Sends network activity to secure server.

SNMP Messaging	Provides instant alerts to management console for pre-set traps.
Limit connections to specific remote systems	Only remote PC's that are explicitly identified can access host PC.

Conclusion

Remote control software provides internal helpdesks and third party support organizations with a cost effective support tool. The ability to gain access to another PC support technicians can diagnose very quickly, resolve problems just in time and update servers without leaving their desks.
But raising productivity could also raise the potential security risks. Microsoft provides the customers with a build in remote control solution that's very easy to user but also has got a lot of vulnerabilities. Even if all vulnerabilities are closed the system is not secure enough for external remote control.
All remote control solutions are to lower support costs and increases user satisfaction with the helpdesk. But, if the proper security features are not available, remote control software could expose PCs and the corporate network to unauthorized access from hackers and disgruntled employees.
Companies need to evaluate and examine carefully the security capabilities of the remote control software they choose. You have to take a look at the security features for administration of a host, the whole network, a server or workstation. Always keep in mind that an unauthorized person could make all the changes which a full administrator could make even you have no proper security in this solution.

References

CERT Security Improvement Modules. "Configure computers for secure remote administration". May 02, 2001.
URL:http://www.cert.org/security-improvement/practices/p073.html (April 20, 2003)

CERT Security Improvement Modules. "Outsourcing Managed Security Services". January 21, 2003.
URL:http://www.cert.org/security-improvement/modules/m03.html (April 20, 2003)

SANS Institute. "How To Eliminate The Ten Most Critical Internet Security Threats". Version 1.33.
URL:http://www.sans.org/topten.htm (April 20, 2003)

IBM Redbooks. "Implementing Tivoli Remote Control in Large Enterprises". SG24-5125-00. May 1999.
URL: http://www.redbooks.ibm.com/redbooks/SG245125.html (April 20, 2003)

Symantec Corporation. "Why should I buy pcAnywhere when the features in Windows XP are free?"
http://service1.symantec.com/SUPPORT/pca.nsf/docid/2001100312495312 (April 20, 2003)

Symantec Corporation. “Addressing Security with pcAnywhere”. March 2001. URL:http://enterprisesecurity.symantec.com/PDF/Addressing_Security.pdf?PID=6642563 (April 20, 2003)

Microsoft TechNet KnowledgeBase “HOW TO: Use IPSec Policy to Secure Terminal Services Communications in Windows 2000”
URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;Q315055&sd=tech (April 20, 2003)

McClure, Stuart. Scambray, Joel. Kurtz, George. “Hacking Exposed”. 1999.
Chapter 8. “Dial-up and VPN Hacking”.
Chapter 12. “Remote Control Insecurities”.

Symantec Security Response Whitepaper: ”Threats to Instant Messaging”
http://securityresponse.symantec.com/avcenter/reference/threats.to.instant.messaging.pdf (April 20, 2003)

Symantec Security Response Whitepaper “Secure Instant Messaging”
http://securityresponse.symantec.com/avcenter/reference/secure.instant.messaging.pdf (April 20, 2003)