Global Information Assurance Certification Paper

NetMeeting 3.01
Remote Desktop Sharing:
Security Concerns

Randy Humphrey
SANS GIAC Practical Paper
Assignment Version 1.4b Option 1
May 20, 2003

Introduction

The growth in the networking and interconnection of systems has blurred the notion of a 'stand alone' system, making physical presence less of a requirement for system operation, access, and maintenance. Here we'll examine the concept of Remote Desktop, in particular analyzing Microsoft's NetMeeting 3.0 Remote Desktop Sharing (RDS) offering. Security features and risks will be covered, as well as recommendations for RDS implementation.

Background: What is Remote Desktop?

Remote Desktop is a model where a distant system 'takes control' of a local system by viewing its desktop session and acting as master for keyboard and mouse input. Unlike traditional remote access methods such as telnet and rlogin, Remote Desktop offers more than a simple text command line interface. If provides the full graphic image of the host (a.k.a. target) machine's desktop, and adds mouse support to the input method. In many instantiations it can even cross architectural boundaries.

The advantages of such access are numerous:

- Telecommuting: The full power and content of a work system could be accessed from a lightweight home machine with only the overhead of the remote desktop tool. The client (remote or controlling) system would be able to access all applications, data, and processing power of the host. Lengthy background processes, such as large software builds, could be checked from home without the need for a drive in.
- Traveling: A work system could be accessed and used from any location with web access, such as hotels, airports, internet cafes, branch offices and customer locations. Forgotten files and presentations can be retrieved.
- Presentations and team events: A group of people could be granted simultaneous access to a system to view presentations, demos and prototypes. Teamwork and collaborative efforts on common files is possible
- Remote assistance and technical support - work on a system from another location, allowing the customer to possibly see the fix
- Systems administration - group/user ID/password management on multiple remote systems from one controlling system

Indeed, Remote Desktop in many cases is nearly as good as being physically at the target machine, except for these limitations:

- Performance: overhead of remote desktop software, network latency
- Can't swap removable media (CDs/DVDs/diskettes)
- Possible limitation to other input means, such as CAD tablets, game controllers, etc.

The biggest challenge for Remote Desktop, though, is one of security. Remote Desktop potentially exposes the machine to virtually unlimited access from a distant controller. How does one assure that the remote access is authorized, intended, and confidential?

In the UNIX sphere this has been accomplished with tools such as SSH and X-Windows. SSH provides strong cryptography to prevent unauthorized access, and X-Windows transforms a simple text interface into a full graphical representation.

For the Windows environment, though, the answer is not as clear. First, a consistent offering has not shipped with the OS for all versions. Aftermarket solutions were lacking in encryption, authentication or other security elements. For others, the implementation required other significant costs [1].

Microsoft's NetMeeting 3.01 RDS - Introduction

Microsoft NetMeeting 3.01 is a tool that supports a variety of sharing and collaboration tools between Windows systems. Primarily used as a real-time teleconferencing aid, it can establish and share video and audio sessions for numerous remote participants. It also provides other community tools such as chat and electronic whiteboard. Attendees can simultaneously share applications and files on the host's system. NetMeeting 3.01 also includes Remote Desktop Sharing, in which a host system can allow for remote desktop takeover from an authorized client.

How NetMeeting RDS Works

To use Remote Desktop Sharing, both host (target) and client (remote) systems start NetMeeting. The host system will first activate NetMeeting, then close it to specify 'Activate Remote Desktop Sharing'. The host is now in a listening mode, waiting for an RDS connection. It is also strongly recommended to log off the host system at this point.

The controlling system now uses NetMeeting to issue a secure call to the host. It specifies the machine name or IP of the host. A dialog box for remote desktop login follows, prompting for administrator name, password, and domain on the host machine. After a few seconds, the host desktop appears on the remote computer's monitor. In the host desktop window on the controller monitor the operator will send a ctrl-alt-del sequence to the host. The operator now has a virtual keyboard and mouse on the host system, and can log on and work remotely.

NetMeeting Security Features

NetMeeting boasts several security features for remote desktop control. Session establishment and authentication/authorization is provided in one of two ways: User authentication or session password. User authentication is achieved by either certificates or user ID/password accounts. Certificates may

be generated by NetMeeting, or by other external and intranet certificate authorities. User authentication may also use a user ID/password account on the local host system. In addition to user authentication, sessions may be established with a distributed session password.

Beyond authorization and authentication NetMeeting offers secure encrypted communication via the T.120 and H.323 protocols. The NetMeeting Resource Kit also offers advanced configuration and features.

Installing and Running NetMeeting Remote Desktop Sharing

- Windows 95/98/ME/NT: NetMeeting isn't part of the base product, but can be installed from http://www.microsoft.com/windows/netmeeting/
- Windows 2000: NetMeeting installs with the base product, and can be accessed by **start->programs->accessories->communications->NetMeeting**
- Windows XP: NetMeeting is included in the full install of Windows XP. However, it doesn't appear on the Start menu until it's activated, apparently by design. To activate NetMeeting:

  1. Click **Start**, then **Run**, and enter **Conf**.
  2. Click **OK**.
  3. In the NetMeeting Wizard, supply the necessary information, and then select the **Put a shortcut to NetMeeting on my desktop** (or on my Quick Launch bar) check box.

  NetMeeting will start, as well as show up in the most frequently used programs list on the Start menu. [2]

NetMeeting Security Risks

NetMeeting RDS, and to some extent remote control software in general, carries several security risks. Most obvious is the power of the tool by nature, that which allows another person both authorized or potentially unintended control of your system. System ownership is transferred to an outside source, and the local owner responsible for policy management gives up control, at least temporarily, of administration and content of the system. Even a benevolent controller can accidentally erase files, install software, or change configuration and settings with adverse effect. Changes made by another may not be logged, making correction and even recognition difficult at best.

Of greater concern are the vulnerabilities that are opened to hostile attempts. Remote desktop systems may be susceptible to unwanted takeover, depending on the tool, configuration, and network configuration such as firewall settings. NetMeeting is without an invalid login threshold, and is potentially susceptible to brute force login attempts. It doesn't set password requirements such as minimum length or expiration time, unless separate Group Policy settings are in

effect. NetMeeting RDS runs as a Windows service, and it's easy to overlook that it's active and waiting for remote connection attempts.

NetMeeting authentication by local administrator account

NetMeeting RDS has the ability to allow establishment of a session by user ID / password authentication. Unlike other remote desktop offerings that have a separate isolated authentication data store, NetMeeting integrates with the local Windows system accounts. Advantages to this approach include ease of use, simplicity, and consistency of accounts, passwords, and privileges. The risk, however, is that it opens possible security holes that go beyond NetMeeting.

For example, by default NetMeeting requires the remote user's ID to have administrator privilege to establish a session. The problem is that the system owner has now allowed another ID with administrative privileges, contrary to the recommendations of most security guidelines. This ID has access that extends beyond RDS, and remains a risk even if RDS is turned off, disabled, or even uninstalled.

Consider the following scenario: A worker in a corporate environment is experiencing a problem, and the remote IT team uses RDS to assist. The IT team requests the creation of a new account ID with administrator authority. The worker creates the account and activates RDS. The IT team completes its work, and the worker disables RDS on their system to prevent further access.

Unfortunately, unless the worker remembers to take the additional step of deleting the 'temporary' user ID, they've created a new vulnerability. There's now a user out there (IT team) that has an account with complete access to the system, and the worker no longer has exclusive control of the system security. Should the user ID be further compromised on the IT team's end the risk increases.

Again, the integration of NetMeeting with Window's local system authentication potentially opens security holes even with RDS disabled or uninstalled. The compromised administrator ID presents an obvious physical exposure, as the perpetrator can walk up to the locked system and logon with full administrator privilege. The risk is far greater with an Administrator account versus a Standard User or Restricted user, as an administrator will typically have rights unavailable to the others. Administrators can add or delete user accounts, modify members of groups, and change user passwords. Checking the **Local Security Settings->User Rights Assignments** of a typical system, administrator had these additional privileges:

- Allow logon through terminal services
- Force shutdown from a remote system
- Manage auditing and security logs
- Modify firmware environment values
- Take ownership of files or other objects

The remote exposure exists as well, as a system administrator ID may gain access in ways outside of RDS. Telnet, rlogin, NetBIOS, RPC, etc. are possible entry points depending on services started and configuration of the host machine, particularly when a valid administrator ID is used in authentication.

Alternatives to local Administrator ID

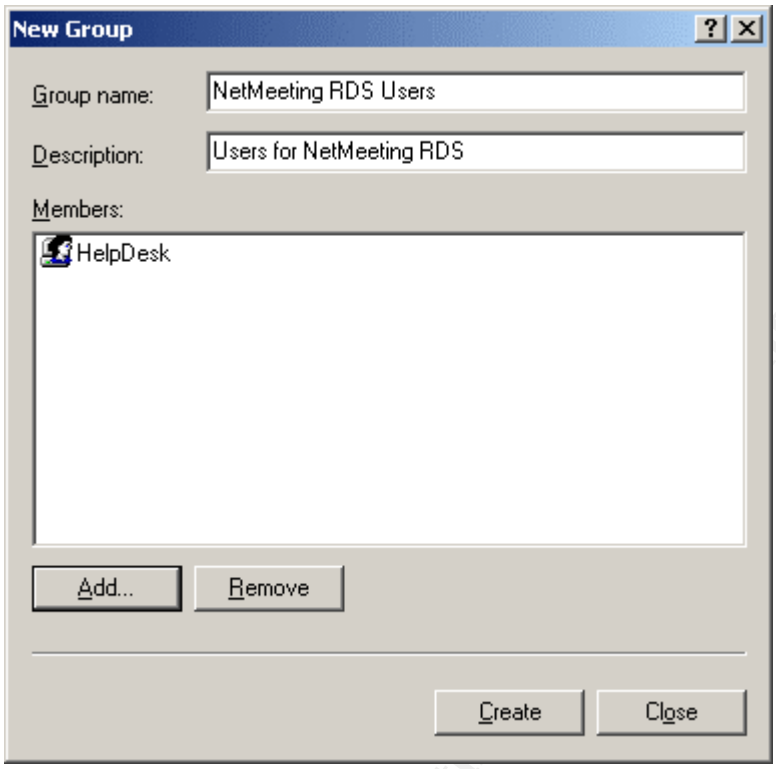
Fortunately NetMeeting provides alternatives to the Administrator permission requirement. Sessions can be established by a user ID without administrator privilege, certificates, and password protection.

User (non-Administrator) ID: There is a way to allow NetMeeting RDS access without requiring Administrator privilege for the ID, though not intuitively obvious or easy to find. According to the NetMeeting 3.0 **readme**:

Administrators can give users the ability to access a computer via Remote Desktop Sharing without giving them accounts with administrator privilege. This can be done by creating a group titled "NetMeeting RDS Users" and adding those users' accounts to that group. [3]

To do this:

1. Click **Start**, **Settings**, **Control Panel**, **Users and Passwords**
2. If you already have an existing ID for RDS access and wish to drop its access below Administrator, follow these steps: select/highlight the user, click the **Properties** button. Click the **Group Membership** tab. You can then select a different permission level, such as Standard user.
3. Click the **Advanced** tab, then the **Advanced** button (Advanced user Management)
4. Select/Highlight the **Groups** folder and select the **Action** menu item, then **New Group**
5. For the 'Group name' enter **NetMeeting RDS Users**. Then **Add** the users you want to grant RDS access.



Certificates: NetMeeting is also capable of authenticating through the use of certificates. Certificates are security objects that are used to determine a user's credentials, and link the owner with a pair of public and private electronic keys used for data encryption and digital signatures. Certificates contain information about the owner, such as name, issuing authority of the certificate and expiration date, and verification of key pair ownership.

NetMeeting can use two types of certificates: NetMeeting certificates and external personal certificates. The NetMeeting certificate is generated automatically at NetMeeting setup. Personal certificates typically are issued by trusted third-party certificate authorities, or by local certificate authorities on a company intranet. Certificates are contained in the user's personal certificate store, and are accessible and shared through the web browser.

Personal certificates are preferable, with third-party certificates garnering the highest level of trust. NetMeeting certificates can establish data encryption, but cannot be trusted to provide user authentication. NetMeeting certificates are used by default, but users may choose and view personal certificates instead to verify authentication [4].

Password protection: If personal certificates and local user accounts are not acceptable means of authentication, another option exists. NetMeeting can establish connections simply using password protection. Here the owner starts

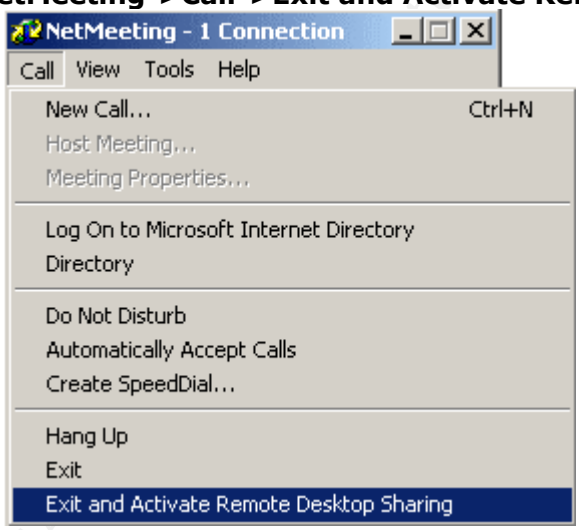
(hosts) a meeting, in the process creating a meeting password. The password is given to the remote controller, and they initiate a connection to the host system.

Note this use of NetMeeting remote support differs from the other methods. Here NetMeeting is active and waiting on a call, and Remote Desktop Sharing is technically disabled ('grayed out'). The remote system places a call to the host, and is prompted for the meeting password. If successfully entered, the host has the option of accepting or declining the connection. Once accepted, the host can go to sharing options and permit access to the desktop. While the authentication mechanism isn't as secure, this approach does allow the host a greater level of control over establishing sessions, and doesn't require Remote Desktop Sharing to be activated in a passive accepting mode.

Using NetMeeting RDS with a User (non-Administrative) ID
The following details how to establish an RDS session using and ID without administrator authority.

From the host (target) machine:

1. Exit NetMeeting and Activate Remote Desktop Sharing:
   NetMeeting->Call->Exit and Activate Remote Desktop Sharing

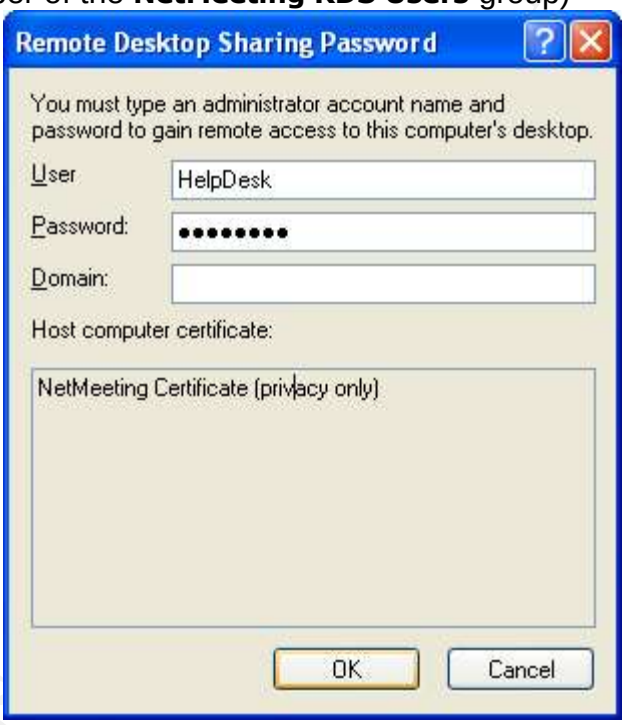


   If NetMeeting is not already running you can also activate from the NetMeeting icon in the Taskbar: right click on the NetMeeting icon, select Activate Remote Desktop Sharing
2. Lock the target machine: **Ctrl+Alt+Del, Lock Computer**

From the client (controlling) machine:

1. Start NetMeeting and place a call (**Call-> New Call** or click the yellow telephone icon). Enter the address of the target machine:

2. Enter the User/Password/Domain of the ID that's granted access (member of the **NetMeeting RDS Users** group)



3. Control is now granted at this point, and the target machine's desktop will appear within a window on the controlling machine. The target machine is locked out from keyboard and mouse input, with the exception of **Ctrl+Alt+Del** or **esc** to force termination.
4. When the controlling machine finishes and wishes to end the session it ends the call from NetMeeting. From the NetMeeting application select **Call -> Hang Up**, or click the end call icon (phone with red arrow down)

NetMeeting IP Ports

NetMeeting requires several TCP and UDP ports to establish connections when calling others. The table below shows the TCP/UDP ports used and their purpose [5]:

Port	TCP/UDP	Type	Protocol	NetMeeting Use
389	TCP	static	LDAP	Internet Locator Server (ILS)
522	TCP	static	ULP	User Location Service (deprecated, use ILS)
1503	TCP	static	T.120	Data conferencing
1719	UDP	static	RAS	Gatekeeper
1720	TCP	static	H.225.0	H.323 call setup
1731	TCP	static	msiccp	Audio call control
1024-65535	TCP	dynamic	H.245	H.323 call control
1024-65535	UDP	dynamic	RTP/RTCP	H.323 streaming (Audio/Video)

To establish outbound NetMeeting connections the firewall must be configured to:

- Pass through primary TCP connections on ports 389, 522, 1503, 1719, 1720, and 1731
- Pass through secondary TCP and UDP connections on dynamically assigned ports (1024-65535).

A TCP port is dynamically negotiated by the H.323 protocol for call control. In addition four UDP ports (inbound and outbound on each side of the firewall) are determined for audio and video streaming. These dynamically negotiated ports are selected arbitrarily from all ports that can be assigned dynamically [6].

Recommendations for NetMeeting RDS Use

Generally speaking, most enterprise environments will chose to avoid the use of NetMeeting RDS and remote desktop applications in general, at least for access beyond their intranet firewall. They'll find any potential benefits to be outweighed by the significant risks incurred and the potential for system corruption and compromised data integrity. Many large corporations already prohibit connections to remote systems outside approved secure gateways as part of their security policy. A remote connection from home or travel location via public internet would most likely violate this policy.

A case can be made, however, for limited temporary access to solve crisis situations. Here the risk/reward ratio may be favorable when costs such as down time, travel, and loss of critical services are taken into account. This is particularly true when the risk is limited to a short window, instead of activated constantly off-hours waiting for connect requests.

For these cases, an enterprise environment might take these precautions:

- Establish a session with an explicit start of a shared meeting, using password protection and certificates for authentication and encryption. This insures temporary access without leaving residual user accounts on the host system.
- If RDS is to be used instead, don't set the RDS service to automatically start. Start it manually on an as-needed basis, and stop the service when the session is complete.
- Avoid creating user accounts with Administrator authority for access. Create accounts with the most restrictive permission possible, and add to the **NetMeeting RDS Users** group.
- If Administrator IDS are necessary, avoid persistent passwords. Change the password at the completion of a session, resetting it for the next intended controller.
- Don't propagate the same RDS user ID/password across the organization. Should this account become compromised the entire organization is potentially at risk
- Give passwords appropriate strength and aging. Preferably update Group Policies on systems to enforce this.
- The user at the host system should ideally monitor all activity conducted by the controller, mindful of suspicious activity. At any time the user on the host side can hit **Ctrl+Alt+Del** or **esc** to terminate the session
- If the host user is not present, the system should be logged off after activating RDS.
- Administrators should use the NetMeeting Resource Kit Wizard to set security settings for all users in the organization, and to prevent users from altering the settings
- Make sure Microsoft patch Q299796 is installed, which fixes a possible Denial Of Service vulnerability in NetMeeting (Bugtraq ID 1798, updated June 22, 2001)

Obviously, there are serious risks involved in letting another user control your system, particularly if given full administrator access. The recommendation is to activate remote desktop only as needed, to know and trust the requesting controller, and be present at the target system to visually check the actions taking place.

However, Jody Weiner [8] points out that even this seemingly secure approach carries significant risk should the controller unknowingly have malicious intents. Even under watchful eye events could take place fast enough to avoid visual detection. For example, a controller might:

- From a Word session use 'save as' to overwrite vital system files
- Use Internet Explorer to download malicious code or a Trojan
- Insert command.com into a Word document in order to gain system access

Other Microsoft offerings

Starting with Windows XP, Microsoft appears to be phasing out NetMeeting in favor of two seemingly similar offerings: Remote Desktop and Remote Assistance. The intended use and security, however, differs from NetMeeting.

NetMeeting was designed as a multi-user conferencing tool, aimed at hosting presentations and discussion groups. It featured the sharing of whiteboards, applications, chat sessions and audio/video presentations. The sharing of the entire desktop was included, presumably to allow live demonstrations of application and system events not easily duplicated in a canned presentation. Sharing control of the desktop was a logical extension, allowing another member to 'take the wheel' for their portion of the demonstration.

Desktop sharing was taken one step further with NetMeeting's RDS. Rather than explicitly starting a conference and sharing the desktop amongst one or many users, RDS allowed a passive or background connection to a single user. RDS allowed the desktop to be shared without explicit activation or confirmation from the user at the host system. This capability gave rise to other uses, such as remote system access and remote assistance.

Remote Desktop and Remote Assistance have shifted the focus away from conferencing and presentation and towards access and assistance. The multi-user group session has been replaced by a single connection. Gone are conferencing capabilities such as group chat, whiteboard (though a clipboard remains), and sharing of specific applications.

Remote Desktop: Remote Desktop is intended for the user who seeks access to the files, applications and network resources on his system from home or while traveling.
Remote Desktop differs from NetMeeting's RDS in the following ways:

- Remote Desktop provides access to local devices and ports on the client machine. Audio will play through the client (remote) machine's speakers. Applications running on the host can have access to printers, serial ports and parallel ports on the client system.
- The client file system is accessible as if it were a network shared drive(s), with no additional network connectivity software or configuration required. This differs from NetMeeting, where files are shared in a push/pull exchange in a specified transfer area.
- Console Lockdown. The monitor, keyboard and mouse of the remote system is disabled for the duration of the client session. NetMeeting, on the other hand, can leave the remote monitor visible and permits keyboard override. This could create a security exposure, allowing unintended viewing of activities or session termination and control.

- The host or remote computer must be running Windows XP Professional. The client can be any Windows machine from Windows 95 and up (98, ME, NT 4.0, 2000, XP and 2003 Server). A client also exists for Mac OS X (version 10.1 or higher).
- Remote Desktop also provides access to any client with a web browser, even if the Remote Desktop client software is not installed. The Remote Desktop Web Connection makes the same functionality available over the web. It requires the host machine to have Remote Desktop Web Connection installed, and to be running as a web server with IIS and Active Server Pages (ASP) enabled [9].

Remote Assistance: While NetMeeting RDS is designed for numerous remote operations (such as sharing, collaboration, and administration), Remote Assistance is exclusively for remote technical assistance. It differs from NetMeeting RDS and Remote Desktop in these aspects:

- Remote Assistance allows both the host (novice) and the client (helper or expert) to control the system at the same time. NetMeeting RDS only allows one active session at a time, meaning the local user is locked out while the remote user has control.
- Sessions are initiated by the novice, and several checkpoints allow the user at the host to terminate session establishment. NetMeeting RDS, on the other hand, can optionally be started in a passive listening mode, allowing the remote system to connect without confirmation.
- The novice initiates the session by instant message, e-mail or file. Instant message requires Windows Messenger, and e-mail requires a MAPI-compliant e-mail account such as Microsoft Outlook or Outlook Express.
- Remote Assistance attaches the controller to an existing session, while Remote Desktop establishes new sessions.
- Remote Assistance offers more options for session control than NetMeeting or Remote Desktop, such as setting maximum session time, permitting only view access with no control, and limiting connections to approved channels/users by restricting access to individuals.
- Both systems must be running either Windows XP or Windows 2003 Server.
- Remote Assistance and Remote Desktop use port 3389 for IP connections. When using Windows Messenger to establish the session, only the outbound connection is used. Since most firewalls allow outbound traffic, its unlikely firewall reconfiguration will be necessary. However, when using the file or e-mail methods to establish connection, the host must be able to receive inbound traffic on port 3389.

Conclusion

The implementation of network security is a constant exercise of assessing risk and benefit. Organizations must continually compare ease of use and power of

network applications and services versus the risk these portals present. This is especially true for remote desktop, where the benefits of telecommuting, file and program access, and remote support and control are weighed against the potential risk of data theft and complete sabotage.

While the typical home user may be comfortable with the risk/benefit ratio, it's highly unlikely that most enterprise environments are, especially if the exposure extends beyond company firewalls to the internet, or persistently activated on the host in passive listening mode.

References

[1] Maj, Artur. "Remote Desktop Management Solution for Microsoft". March 18, 2003. URL: http://www.security-portal.org/infocus/1677 (March 2003)

[2] Aljandali, Nahel. "Activate NetMeeting". December 3, 2001. URL: http://www.microsoft.com/windowsxp/expertzone/tips/december/aljandali1.asp (March 2003)

[3] Microsoft. "Windows NetMeeting 3 Readme Text File Contents". October 2, 2001. URL: http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B241159 (April 2003)

[4] Microsoft. "Chapter 5 – NetMeeting Security". TechNet Home, Products and Technologies, NetMeeting. Date not specified. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/netmting/reskit/netmtg3/part2/chapter5.asp (March 2003)

[5] Pouseele, Stefaan. "Using NetMeeting and the H.323 Gatekeeper as a HelpDesk tool". Nov 01, 2002. URL: http://www.isaserver.org/articles/Using_NetMeeting_and_the_H323_Gatekeeper_as_a_HelpDesk_tool.html (March 2003)

[6] Microsoft. "NetMeeting Resource Kit Chapter 4. Firewall Configuration". December 10, 1999. URL: http://www.microsoft.com/windows/NetMeeting/Corp/reskit/Chapter4/default.asp (May 2003)

[7] SecurityFocus. "Microsoft NetMeeting Remote Desktop Sharing DoS Vulnerability". June 22, 2001. URL: http://www.securityfocus.com/bid/1798/info/ (May 2003)

[8] Weiner, Jody. "NetMeeting Security Concerns". July 23, 2001. URL: http://www.sans.org/rr/win/netmeeting.php (March 2003)

[9] Microsoft. "TechNet Resource Kits. Chapter 8: Configuring Remote Desktop". Date not provided. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/reskit/pree_rem_fhca.asp (May 2003)

Shenton, Chris. "NetMeeting Security Concerns and Deployment Issues". October 4, 1998. URL: http://www.shenton.org/~chris/nasa-hq/netmeeting/ (April 2003)

Devx.com (various editors). "NetMeeting 3.x FAQ, tips, and troubleshooting guide by the NetMeeting Zone's editors". June 16, 2000. URL: http://archive.devx.com/netmeeting/nm3_faq.asp (April 2003)

Thompson, Troy. "Using NetMeeting to remotely control desktops". April 28, 2000. URL: http://www.networking.earthweb.com/netsysm/article.php/623391 (April 2003)

Fogie, Seth. "Windows XP Remote Assistance". August 9, 2002. URL: http://www.informit.com (May 2003)