Global Information Assurance Certification Paper

NetMeeting Security Concerns

As the business world depends on digital forms of communication, computer based collaboration tools are becoming more frequently used. One of the more common tools used in business environments is Microsoft's NetMeeting, which is offered for free and provides real-time collaboration tools. Some of the tools provided by NetMeeting include: video/audio conferencing, whiteboard, chat, file transfer, program sharing, remote desktop sharing, and security. Users from inside or outside of a private network are able to connect to each other and utilize the program. A few of NetMeeting's features are of concern in respect to network security. Perhaps, the scariest element is remote desktop sharing; however Microsoft lists security as one of NetMeeting's features. In this paper I'd like to explore how NetMeeting works and understand its security implications in a business environment.

Most companies use a firewall as part of their perimeter defense. The firewall is a system designed to prevent unauthorized access to or from a private network. Because NetMeeting allows connections from outside of the network, the perimeter defense can be bypassed in three ways. The first is via social engineering. The second is holes or vulnerabilities created in the firewall configuration to allow NetMeeting to operate. Lastly, bugs in the program itself can cause security issues. In the following paragraphs, we will explore each issue.

Social engineering is the science of manipulating people to gain access to information or systems that are normally available only to privileged users. It relies on humans, possibly the only far-reaching vulnerability regardless of hardware, software, or network. We often hear about hackers using social engineering to get passwords or credit card information from AOL Instant Messengers users. They do this by pretending to be administrators and requesting information from the user in order to fix a problem with their account. This type of deception is also possible with NetMeeting. The issue with these types of programs is the fact that the identity of the users is not reliable. It is extremely easy to forge a user account since the information is not authenticated in anyway. Additionally, anyone can sit down as someone else's workstation and log on as them. How much damage can a hacker do to your network via social engineering in NetMeeting?

Let's look at a some possible situations. Scenario 1: An executive at your company establishes a NetMeeting connection with a "trusted buddy." The buddy convinces exec to turn on remote desktop sharing so he can fix a problem or make the computer run faster. The hacker now has complete access to everything on the system and possible network resources if the exec is logged onto the network. Scenario 2: The buddy convinces exec to turn on file sharing so he can send him an important document. This document contains a Trojan horse or other malicious program that will give the hacker access to the system later. These two instances show possibilities of major breaches that are caused by the weakest link in network security, the user. Let's look at some of the issues related to allowing NetMeeting traffic to pass through a firewall.

Earlier in this paper we read about firewalls and how their role is to prevent unauthorized access to a network. The way, in which the prevention process works, depends a lot on security policy

within an organization. NetMeeting uses a large variety of protocols and ports. In order for the software to function correctly holes need to be punched in the firewall. This means ports need to be opened. Unfortunately, when a port is opened for NetMeeting, it also allows other types of traffic through the hole. Below is a table listing including the protocol, port numbers, and port types required for NetMeeting to be fully functional.

Port Number	Port Type	Protocol	NetMeeting Use
389	TCP, static	LDAP	Internet Locator Service (ILS)
522	TCP, static	ULP	User Location Service (obsolete after NM ver. 1.0)
1503	TCP, static	Imtc-mcs	T.120 data collaboration
1720	TCP, static	H323hostcall	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 audio/video stream

Excerpt from Mitre report which can be requested @ http://collaboration.mitre.org/leong/netmeeting.htm

You'll notice that the last two rows of this table list dynamic ports. This means when connecting, NetMeeting randomly picks ports from the range of 1024-65535. In that case 64,511 ports need to be opened just to allow two of the program's services to run. On the other hand, you'll also notice that the other 5 services use only 1 port each. One way to limit the possible ways to exploit your network is to disable ports 1024-65535. This will stop the audio and video conferencing portions of the program and only allow text-based traffic. This does also severely limit the capabilities of NetMeeting. Are there ways to use NetMeeting in a more secure fashion?

First let's look at how a normal packet filtering firewall might work. When a TCP/IP packet comes through, the firewall filters based on information in the packet header. Information contained in the header includes protocol type, source address, source port, destination address, destination port, and flag information. With H.323 the source and destination ports are embedded in the packet itself and not in the header, because it is written in ASN.1 syntax. Since the packet filter only knows about what is in the header, it difficult to filter these packets because it cannot find the information needed to function properly. This means packet filtering cannot help secure NetMeeting connections. (For an in-depth explanation, http://www.codetalker.com/whitepapers/h323insecurity2.html)

The only other solution to securing your NetMeeting connection using H.323 is a VPN. A virtual private network is an encrypted point-to-point connection. Mitre completed a study on whether it is possible to limit the ports opened on the firewall and still allow NetMeeting's audio and video capabilities to operate via a VPN. They first tested a hardware-based solution, Timestep VPN. They successfully implemented it by opening only 2 ports. They also tested some software based VPNs, but these were not as successful. Use of NetMeeting within a VPN can limit many security risks to both the user and the network. However, it still necessary to explore

security shortcomings within the software itself. There are multiple versions of NetMeeting. Since the majority of users will be downloading the newer version, I have chosen to concentrate on issues within NetMeeting version 3.

One issue addressed earlier in this paper is that fact that logon credentials are not verified and thereby allow very little proof that you are connecting with the correct person. Another issue related to this is within they way NetMeeting enables users to find each other. This done using Directory Server that lists all of the users who are logged in to NetMeeting. The server can be on your local network or on the Internet. Once a user logs on to the Directory Server they are logged on indefinitely, even if they exit NetMeeting. In order to log off the server a user must click on the "Call" menu and choose log off "server name". The problem with this is when a user doesn't log off, it is possible for someone else to sit down at their workstation and act as them. This makes the issue of user authentication even more insecure.

Another vulnerability in NetMeeting is part of the new security features that Microsoft has added to version 3.0. The person hosting the meeting is now able to require a password from entrants to the meeting. Unfortunately, there are no password requirements set and no ability to lock a user out of the meeting after failed attempts. Without requiring a minimum password length, numbers, and special characters a cracker may find NetMeeting users a very easy target. Another result caused by this is possible compromising of more secure network resources. Suppose as a network administrator you have a password policy that requires strong passwords, but you also allow NetMeeting to run in your office. If a NetMeeting password is compromised and other features of NetMeeting are enabled such as remote desktop sharing, then so are your network resources.

NetMeeting version 3 also has new features that include encryption via a NetMeeting certificate and authentication/encryption via a personal certificate from a third party authority. Mitre thoroughly tested these capabilities and found a major flaw. NetMeeting cannot differentiate between a user with an encrypted connection and a user with an authenticated/encrypted connection. This means that although a NetMeeting host may require security, there is not way to tell if the user is authenticated via their certificate. Mitre also found that the security features were not reliable. During their tests, there were times when NetMeeting did not act as though security was turned on even when it was activated. At other times it worked normally. It also important to note that when then encryption feature is enabled for a secure call, audio and video are turned off. This is because of the H.323 protocol that was discussed earlier in this paper. A meeting host can add a bit more security to their workstation by limiting what participants can do in a meeting. These feature include: requiring a secure connection, only allowing the host to allow incoming calls or place outgoing calls, and only the host can start other collaborative features (ex: sharing).

During a meeting, it may be useful to enable sharing. This feature allows someone to open a document in a program such a Microsoft Word and share it with other meeting participants. By default, if a participants wishes to take control of the document they must request permission from the owner of the document. However, it is possible for the owner to automatically accept requests for control. In order for the owner to take back control during any part of the session, all

they need to do is press the esc key. This feature has some major security risks. One is that the controlling user has full access to the application and all of its features and all resources on the machine including network drives. Let's look at a few scenarios. Scenario 1: Controlling participant in Microsoft Word, uses the "save as" feature and overwrites import system files on the host computer. Scenario 2: Controlling participant in Internet Explorer downloads malicious code or a Trojan to the host machine. Scenario 3: As in Chris Shentons' article, the controlling participant in Microsoft Word inserts command.com into the document. Next they have shell access to the system and can delete files, FTP new programs, ect.

According to Chris Shenton, Microsoft's response to these security flaws is that there is an assumed amount trust between NetMeeting users and that participants must be diligent in watching what is happening to their machine. In Chris' test, they were able to insert command.com and begin deleting files within 10 seconds from the host machine. Is this enough time for the average user to see what it happening and take control back? In some cases maybe it is possible to notice the enemy in such a short period of time, but in many other cases it is not. This brings me to my next point. In order to decide how to deploy NetMeeting you need to take into account your unique environment and implement a security policy based on those needs.

All companies are not the same and may not require similar levels of security. For example, the FBI may find that unencrypted voice and video as well as other vulnerabilities in NetMeeting make it a product that cannot be used in their environment. However, Uncle Jim's Video Store franchise may not have any problem implementing all of NetMeeting's security features. In this last section of my paper, I would like to make some general NetMeeting security suggestions.

If there is a definite need to utilize NetMeeting in your environment, but you are concerned about users turning on sharing features there is a solution. Microsoft provides a NetMeeting Resource Kit, which allows you to customize the program using policies. Some of the things you can do include: disable sharing, disable automatic call answering, require users place and receive encrypted calls, and prevent users from implementing audio/video features. By creating policies with the Resource Kit, you implement the program in a more secure fashion. However, keep in mind that users can bypass policies by disconnecting from the network.

There are other ways to secure NetMeeting besides the Resource Kit. The following list is taken from Mitre's study on security within NetMeeting. Many these items have been covered early in the paper.

NetMeeting Security Checklist

1. Require use of security
2. Require use of personal certificates for both encryption and authentication
3. Disable use of Audio and Video unless using it across a VPN
4. Place restrictions on what programs can be shared using NMRK (Resource Kit)
5. Require all collaboration take place in attended mode
6. Disable use of Remote Desktop Sharing feature.

Item number 1: Although, you cannot enforce the password requirements in NetMeeting, it should be company policy that user implement strong passwords with minimum length requirements. Additionally, users should avoid words or names and include numbers and special characters to heighten the security level of their passwords.

Item number 2: Encryption will decrease the ability of someone intercepting the data.

Item number 3: This can be done at the application level via the Resource Kit or manual configuration. However, it can also be implemented at the firewall level by closing ports 1024-65535 for both TCP and UDP. This will limit the available entry points for hackers into your network and disable the features of NetMeeting that cannot be encrypted.

Item number 4: Restricting the shared programs to only ones that are needed in your organization can cut down on security risks. If you do not need access to a command prompt or Internet Explorer then, this can limit what an attacker could do.

Item number 5: No one should give control of a document to another user without watching what is being done.

Item number 6: Remote Desktop Sharing was only briefly discussed in this paper for one reason. In most environments this feature is not needed and should be disabled. I felt it was more important to focus on security issues within the more commonly used business features of the program. Enabling desktop sharing is a major security risk; you are giving complete control of your machine to another user if you enable this feature.

The object of this paper was to explore how NetMeeting works and understand its security implications in a business environment. We've looked at what ports the program utilizes when being accessed through a firewall, the viability of packet filtering to secure the program, human aspects of the program including social engineering, and security flaws in the program itself. NetMeeting is an extremely powerful tool for use in the business environment. However, it is important to understand the security caveats in the program and take the necessary steps to limit the damage that malicious users can achieve. This paper has highlighted some of the more dangerous aspects of the NetMeeting. For more in-depth information, visit my references. Mitre has a very thorough study, which includes screen shots and configuration info as well as more security flaws in NetMeeting. This can be requested from the excerpt listed on the Mitre site below.

References

Shenton, Chris. "NetMeeting Security Concerns & Deployment Issues." 4 October 1998. http://www.shenton.org/~chris/nasa-hq/netmeeting/ (July 2001)

Excerpt from Mitre study: "Security of the NetMeeting Collaborative Tool." http://collaboration.mitre.org/leong/netmeeting.htm (July 2001)

Microsoft product information page: http://www.microsoft.com/windows/NetMeeting/default.ASP (July 2001)

Code Talker. "Designing For Insecurity." http://www.codetalker.com/whitepapers/h323insecurity2.html (July 2001)

Packet Storm Security. "People Hacking: The Psychology of Social Engineering." 7 May 1997 http://packetstormsecurity.org/docs/social-engineering/aaatalk.html (July 2001)

"H.323 and Firewalls: Problems and Solutions." 25 January 2001 http://www.surfnet.nl/innovatie/surfworks/showcase/h4.html (July 2001)