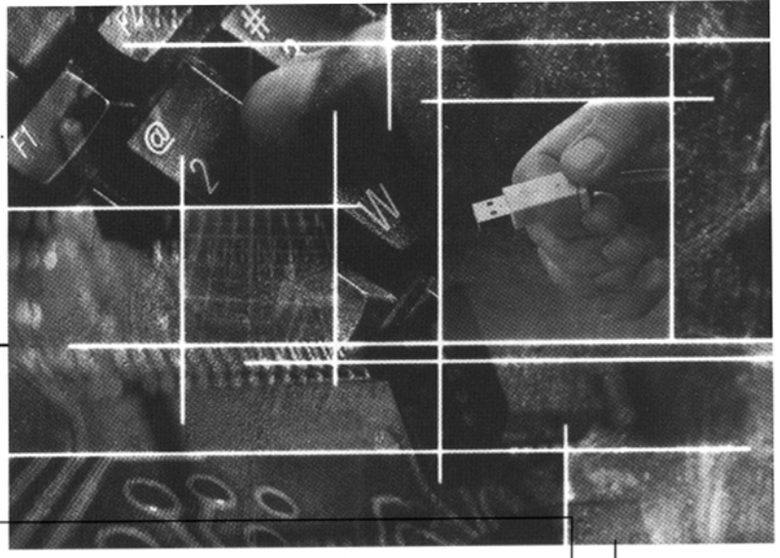

NetMeeting 的网络安全问题研究

韩潇毅 李之棠 (华中科技大学计算机科学与技术学院 430074)

摘要：本文先就NetMeeting使用中带来的网络安全问题做了详尽的分析，特别指出了NetMeeting对防火墙的影响。随后提出了四种解决方案，其中重点介绍了防火墙＋网关解决方案和VPN解决方案。

关键词： 网络安全 NetMeeting 防火墙 VPN

1 引言

Internet的发展改变了人们的工作方式，微软开发的NetMeeting网络会议软件使人们可以通过Internet进行可视通话和数据会议。人们可以在计算机上看到通话者的影像；也可以进行网上聊天、共用电子白板或相互传输文件；甚至可以共同编辑一份WORD文档。然而人们在使用这些方便功能的同时，也使自己的系统乃至整个内部网络暴露在黑客的攻击下。黑客可以截获通信内容、假冒信任用户、远程控制计算机；更危险的是为允许NetMeeting通过，防火墙有可能处于一种非常不安全的配置状态，使整个内部网络出现安全漏洞。

2 NetMeeting带来的安全隐患

NetMeeting使用起来非常方便，然而正是这种易用性暴露出来许多安全隐患，其中主要有三个：

(1) 数据的机密性、完整性及用户的真实性无法保证；

(2) 参加NetMeeting的主机可能受到不安全的远程控制；

(3) 削弱了防火墙的控制功能并暴露内部主机。

2.1 数据的机密性、完整性及用户的真实性无法保证

在默认方式下，NetMeeting网络会议是没有安全保证的：

(1) 没有用户身份验证；

(2) 数据会议的内容没有加密；

(3) 音频/视频流数据没有加密。当用户按照默认方式使用NetMeeting通信时，黑客很容易监听到通信的整个过程，并从中得到与会者的IP地址、个人信息、在目录服务器上的注册信息以及通信内容。在以后的通信过程中，黑客就有机会伪造通信一方的IP地址，假冒成信任用户来获得更多的敏感信息。一旦假冒成功，黑客将会首先使用NetMeeting的远程控制功能控制用户的计算机，再留下后门或注入木马程序，并进一步以此为基础打开内部网的大门。

2.2 不安全的远程控制

NetMeeting的远程控制功能十分强大，它允许用户将自己计算机上正在运行的程序进行“共享”，共享后的程序可以被所有的参与者控制。这种远程控制十分危险，程序所有的权限都被远程用户所拥有，如果该程序可以向硬盘写文件，本机的系统文件就有被改写的可能；如果该程序可以发电子邮件，黑客可以利用它将敏感信息通过电子邮件发出；如果Windows桌面被共享，黑客就能以当前用户的身份控制整个计算机，这个身份往往允许访问内部网络上的其他服务，这时黑客已经渗透到内部网络之中了。

2.3 削弱了防火墙的控制功能并暴露内部主机

防火墙是一个安全网络的唯一出口，为了让网络内的用户能同Internet用户进行NetMeeting通信，必须对防火墙进行相应的配置。由于NetMeeting的每一种功能都对应了一个标准，有些标准还相当复杂，配置防火墙时不可避免的会造成防火墙防御功能削弱。下表列出了NetMeeting使用的标准：

标准名称	端口号	端口类型	用途
LDAP 目录服务标准	389	静态 TCP	Internet 目录服务器
T.120数据会议标准	1503	静态 TCP	NetMeeting 数据会议
H.323音频/视频会议标准	1720	静态 TCP	H.323
	1731	静态 TCP	
	1024–65535	动态 TCP	H.245
	1024–65535	动态 UDP	RTP/RTCP /

对于LDAP目录服务标准和T.120数据会议标准只要在防火墙上开放相应的端口就能配置成功，但是在防火墙上配置H.323音频/视频会议标准则会带来两个安全漏洞。这都是由H.323动态协商端口造成的：

如上表所示，H.323协议族的H.245和RTP/RTCP协议使用的端口号是在通信初始化阶段由通信双方动态协商确定的，防火墙无法预先知道。为使H.323协议通过，防火墙必须开放双向1024－65535的TCP/UDP端口。如果这样配置，内网的这些端口都会暴露在黑客的攻击下，而防火墙就像一个纸老虎。

H.323标准给防火墙带来的另一个问题是：NAT（网络地址转换）无法使用。防火墙往往通过NAT隐藏内部网络的拓扑结构。因为无法参与NetMeeting的端口协商，对发向内部主机动态端口的包，防火墙会认为是无效的包而忽略。这也是NAT用户使用NetMeeting时听不到Internet用户声音的原因。为使双方都可以听到或看到对方，必须把NetMeeting主机配成外部地址（Internet地址），这样做带来的问题是——内部主机被暴露了。

3 解决方案

针对前面提到的一些安全隐患，存在着不同安全级别的解决方案。其中包括：提供初级安全功能的NetMeeting安全呼叫和Windows域策略控制；提供中高级安全功能的防火墙＋NetMeeting网关解决方案；提供最高安全特性的VPN解决方案。

3.1 使用安全呼叫避免窃听或假冒信任用户

NetMeeting自身提供了与ITU T.123B标准兼容的安全机制为数据会议提供安全保证，该标准包括T.224安全呼叫协议。使用T.224安全呼叫协议，呼叫者和接受者交换公钥，并使用各自的私钥为发出的数据加密。使用安全呼叫使得假冒信任用户或截获通信数据变得非常困难。

但是安全呼叫只具备初级的安全功能，它有下面几个缺陷：

(1) 仅仅对数据会议部分加密，而没有对音频/视频数据加密；

(2) 进行音频或者视频会议时则无法使用安全呼叫模式；

(3) 没有解决其他两个安全隐患。

3.2 使用Windows域策略编辑器禁止远程控制

使用域策略可以关闭NetMeeting的某些危险功能。微软提供了一个针对NetMeeting的系统策略模板，该模板提供了允许或禁止NetMeeting各种功能的详细选项，如文件传输、应用程序共享、音频/视频的使用、存取目录服务等等。网络管理员可以使用这些选项限制那些不安全的功能，以达到整个网络安全的目的。

然而域策略只能实施在注册到主域控制器的计算机上，对于那些独立于域的计算机则无法控制。因此在网络管理比较松散的环境中，仅使用域策略无法保证整个网络的安全。

3.3 使用应用网关加固防火墙并隐藏内部主机

为使现有的防火墙安全地支持NetMeeting，可以在内部网部署一台NetMeeting应用网关（代理服务器）。NetMeeting应用网关可以直接被外部访问，它是一个H.323/T.120网关，具备认证、访问控制能力。只要在防火墙上为网关开辟专门的通道，它就可以将合法的NetMeeting通信流量通过防火墙与外界交互了。这样防火墙只需为网关打开动态协商范围之内的端口，隐藏了内部主机，同时可以在网关上对远程控制进行限制。下面是联合使用FW3000防火墙和WinProxy代理服务器的一个案例。

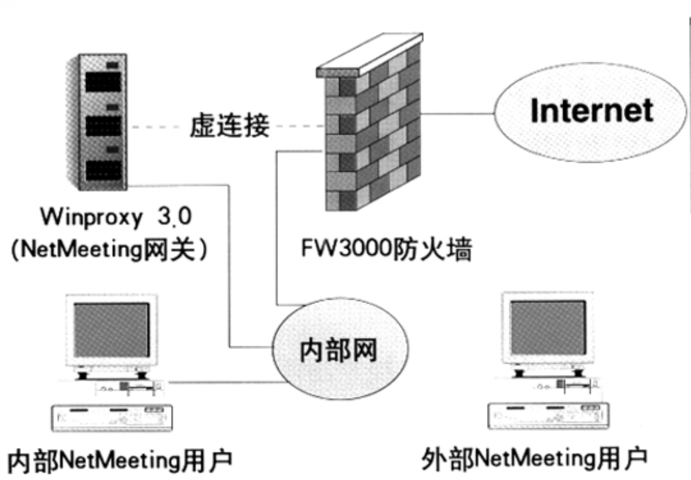

图 1 防火墙＋网关解决方案

如图1所示，WinProxy代理服务器配有两块网卡，一块使用内部地址接入内部网，供NetMeeting客户端连接使用；另一块使用外部地址与防火墙的虚拟网卡相连，

构成虚连接。FW3000防火墙使用特有的透明和虚连接技术为WinProxy开辟了一个通向Internet的专用安全通道，这个通道只允许NetMeeting流量通过。这样内网用户就可以使用WinProxy作为NetMeeting网关来与Internet用户通信了。

使用NetMeeting网关可以杜绝大部分安全漏洞，但是仍然暴露了作为网关的计算机，而且实施起来比较复杂。为了简单、安全地使用NetMeeting，VPN是最佳选择。

3.4 VPN——最终解决方案

VPN(虚拟专用网)将两个或多个物理上分开的网络连接成一个安全的虚拟专用网，经常用于将各分支机构的网络通过Internet相连。如VPN2000就是一个非常优秀的VPN产品，它具有安全强度高、简化网络结构、配置灵活、与防火墙结合紧密、对用户透明等特点。针对NetMeeting应用，局域网和Internet用户之间可以使用相应的VPN设备建立隧道，隧道建立成功后，用户之间的通信就像在同一个内部网络之中，不需要任何特殊的设置。即使用户之间跨越多个网络，经过VPN设备加密过的用户数据几乎是不可能被破译的。由于黑客根本无法进入隧道，也就没有任何进入内部网络的机会，这就从根本上杜绝了任何不安全的因素，给内部网络以最大的保护。VPN的使用也使NetMeeting应用最为方便，因为用户不必为使用NetMeeting做任何特别的设置。下面是使用VPN2000的一个案例(见图2)。

如图2中所示，VPN2000隧道加密机结合在FW3000防火墙中，它与Internet用户计算机上的端用户VPN软件共同创建了一条隧道，从而构造了一个临时的虚拟专用网。原内部网用户和Internet用户可以使用内部地址进行NetMeeting通信，就如同内部网用户之间通信一样。

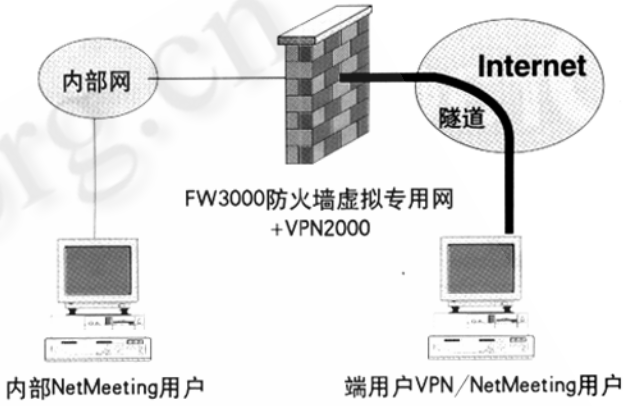

图 2 VPN解决方案

4 结论

本文就NetMeeting的使用指出了不安全的因素，然后使用了目前流行的网络安全解决方案对这一应用进行了支持。对于需要在Internet上使用NetMeeting的用户有一定的指导作用；对于网管人员也有一定的参考价值。由于入侵与反入侵技术的不断发展，也由于作者知识有限，可能仍然存在其他安全漏洞没被发现或者存在更好的解决方案，作者将在以后继续关注这方面的发展。■

参考文献

1 Microsoft Corporation. Microsoft NetMeeting 3.0 SDK [M]. 1999。

2 Chris Shenton. NetMeeting Security Concerns and Deployment Issues [EB/OL]. 1998。