网络安全隐患与防范措施

□袁国民

随着网络经济和网络社会时代的到来，网络将会进入一个无处不有、无所不用的境地。经济、文化、军事和社会活动将会强烈地依赖网络，作为国家重要基础设施的网络的安全和可靠将成为世界各国共同关注的焦点。而Internet原有的跨国界性、无主管性，不设防性、缺少法律约束性，为各国带来机遇的同时也带来了巨大的风险。为了使Internet/Intranet在我国能健康地发展必须要重视这些风险和冲突。

关健词：网络网络安全信息安全措施

信息既是一种资源，也是一种财富。随着知识经济时代的到来，保护重要信息的安全，已经成为全社会普遍关注的问题。有资料表明，目前在互联网上大约有将近20％以上的用户曾经遭受过黑客的困扰。尽管黑客如此猖獗，但网络安全问题至今仍没有能够引起足够的重视，更多的用户认为网络安全问题离自己尚远，这一点从大约有40％以上的用户特别是局域网用户没有安装防火墙(Firewall)便可以窥见一斑。特别从最近发作的几起网络病毒对网络系统及网络安全所造成的危害来看，网络的安全隐患十分严重，不得不引起大家的足够重视，本文就网络安全与防范措施谈点看法。

网络既是信息共享的场所，同时也是信息安全隐患最突出的场所

随着国民经济信息化的迅速发展，人们对网络信息安全的要求越来越迫切，尤其自Internet得到普遍应用以来，信息系统的安全已涉及到国家主权等许多重大问题。据统计，在所发生的事件中，有32％的事件系内部黑客所为。另外，据美国国家电脑安全协会（NCSA）的调查表明，近期在各企业的病毒感染案例中，有近一半来自网络中的电子邮件。

目前，我国大多数机关、院校都在其内部建立了Intranet，并通过电子邮件、网关和防火墙与全世界的Internet相联。入网内部的文件很容易受到病毒的感染，这些带毒的文件被执行后，整个的网络很快也会受到株连，从而导致数据丢失，甚至造成网络瘫痪。最近出现的Redcode和nimda两种病毒其传播速度之快和传播范围之广，出乎网络界从业人员的意料，所造成的危害令人十分震惊，大部分系统受到及其严重的干扰，影响到教学和训练的正常进行。

在因特网上，电脑黑客的破坏力非常大：轻则窜入内部网内非法浏览资料；重则破坏、篡改在因特网上存放的软件与机密文件。他们刺探商业情报，盗取巨额资金，破坏通信指挥，盗窃军事机密。因此，你在因特网上收发电子邮件或传送文件时，应特别注意是否有电脑黑客正躲在暗处悄悄作策。

黑客技能主要有：破解密码和口令字，制造并传播计算机病毒，制造逻辑炸弹，突破网络防火墙，使用记录设施窃取显示器向外辐射的无线电波信息，等等。在Internet上黑客使用的工具很多，目前已发现BO（BACKORIFICE）、NETBUS、NETSPY、BACKDOOR等十几种黑客程序。如Rootkin软件就具有特洛伊木马、网络敏感、轨迹跟踪的功能。

黑客的攻击手法主要包括：猎取访问线路，猎取口令，强行闯入，清理磁盘，改变与建立UAF（用户授权文件）记录，窃取额外特权，引入"特洛伊木马"软件来掩盖其真实企图，引入命令过程或"蠕虫"程序把自己寄生在特权用户上，使用一个接点作为网关（代理）连到其他节点上，通过隐蔽信道突破网络防火墙进行非法活动等。

黑客在网络上经常采用的攻击手法是：利用UNIX操作系统提供的Telnetdaemon、FTPdaemon、Remoteexecdaemon等缺省帐户进行攻击；用命令Finger与Rusers收集的信息不断提高自己的攻击能力；利用Sendmail；采用Debug、Wizard、Pipe、假名进行攻击；利用FTP采用无口令访问进行攻击；利用NFS进行攻击；通过WindowsNT的135端口进行攻击；及利用XWindows进行攻击等。

“拒绝服务”是一种破坏性的攻击。这种攻击最早由"电子邮件炸弹"引发，当用户受到它的攻击后，就会在很短的时间内收到大量的电子邮件，使网络系统不能正常工作，严重时会使系统死机、网络瘫痪。后来制造的"信息炸弹"更具破坏威力，信息炸弹一旦爆炸，就会引起网络系统死机。

随着工具软件的丰富与完善，黑客的攻击手段还在不断翻新。由于黑客程序可被植入计算机系统，而不被人察觉，一旦计算机被黑客程序潜入，黑客就可与它里应外合，使其攻击变得十分容易。根据一个专门从事Internet安全监测的机构的统计，对网络攻击法80％是网络管理员未能察觉的。虽然你制止不了黑客的攻击，但你可以使用各种有效的方法追踪这个破坏者。因此，尽快防范黑客入侵已成为计算机领域的当务之急！