网络安全

安全故事

狄登峰 主编

目　　录

网络安全最薄弱环节乃人为漏洞

著名黑客凯文.米蒂尼克(KevinMitnick)日前在接受采访时表示，网络犯罪现已成为影响日益深远的社会问题。尽管很多公司采取了安全防护措施，但这些安全措施在网络犯罪面前仍然显得不堪一击，原因在于他们忽略了网络安全的一个最为薄弱的环节——人的安全意识。

事实上，网络安全最薄弱的环节不是系统漏洞而是人的漏洞。

今年 4 月，1600 多名企业 IT 人士聚集在旧金山的莫斯康中心，聆听前著名黑客凯文.米蒂尼克(KevinMitnick)有关计算机犯罪的报告，米蒂尼克目前已成为一个安全专家和法律专家小组的成员，他要讨论的问题之一是企业否应该雇用前黑客来保障他们计算机网络安全，这是个业界正在激烈争辩的问题。包括惠普公司首席安全战略官埃拉.温克勒(IraWinkler)在内的许多技术大亨们都对此问题颇有兴趣。温克勒不主张雇用黑客负责企业的网络安全，但米蒂尼克反驳他说：“我与他有很多私人交往，我知道埃拉自己以前就是个黑客。”

米蒂尼克曾是世界上最“臭名昭著”的黑客，他曾潜心钻研 15 年，研究侵入世界最大的技术公司的内部系统，为此，他还坐了 5 年的监牢。在重获自由后，米蒂尼克洗心革面，创建了一家安全咨询公司，为客户提供安全防护服务，阻止其他黑客盗用诸如信用卡账号、医疗记录和交易记录的秘密信息。米蒂尼克认为，由于互

联网的迅速普遍，黑客攻击已经呈现出爆炸式的增长，虽然他自己以前发动攻击只是为了好玩，但现在很多攻击的目的却远不止此，它们的目标更多地锁定在了机密的商业和个人信息，目的是为了获得非法利益。甚至连恐怖分子也有可能利用互联网发动袭击，使一些重要的安全系统陷于瘫痪。

面对这些潜在的巨大威胁，政府和许多企业都投入了大量的财力和物力用于安全防范，预计今年一年投入的资金将高达 135 亿美元，比 2000 年翻了一番。但仅仅购置安全软件是远远不够的，政府和企业必须充分注意到人的因素，因为最薄弱的环节很可能是大意的人们，而不是软件的漏洞，米蒂尼克自己攻陷了许多极为繁复的网络，靠的不光是高超的技术，更多的是利用人的弱点。他的名言是："愚蠢是没有补药的！"

米蒂尼克认为，计算机和解调器都不是问题的关键，人才是最重要的，只有把人的安全防范意识提升到一个相当高的地步，黑客攻击的破坏性才能够从根本上降低。米蒂尼克曾假扮过一个摩托罗拉公司的员工，并成功地说服该公司的一名工程师将最新的电话系统软件发送给他。

美国专训反黑高手的黑客学校

长长的鬓角，一小撮山羊胡子，加上一顶黑色的棒球帽——如此打扮的拉尔夫·埃切门迪亚似乎全然不同于传统讲师的模样。不过他确实正在授课，只不过讲授内容是黑客技术。不少学生甘愿支付高额费用来到这家

位于洛杉矶的黑客学校里学习黑客技术，他们的任务是与黑客斗法，防范黑客攻击。

内容：黑客技术

据路透社 29 日报道，埃切门迪亚任职的学校如同一个网络技术高手训练营，支付 4000 美元学费后，学生将在为期一周的时间里学习如何试图攻击并中止别人的网络系统，关键在于如何取得成功。埃切门迪亚说："令人惊讶的是，那些大公司的站点是多么不安全，而更令人惊讶的是，攻击它们是多么的容易。"

学生们告诉记者，所学内容非常实用。在第一天，他们被教授一些基本知识，以及技术研究手段等，这包括搜索引擎和安全数据库等相关知识。掌握这些知识，他们就能够对一些网站的系统及运行维护情况等有所了解。

在老师的点拨之下，学生们只要付出小小努力，便能举一反三。他们能够发现一些公司在继续使用一些早已知道容易受到攻击的有安全漏洞的系统，甚至还能从网上辗转发现某些公司的主管在运营网站的同时还有着自己的一个关于吉他的专门站点等。

目标：黑客证书

尽管入门并不难，但学生要想学习完这些短期课程顺利结业，并如愿拿到结业证书，也并非易事。学生们需要学习一堆诸如对称与非对称加密、传输控制协议端口和服务等专业技术知识。

在学习结束之际，学生还要参加一场由电子商贸咨询国际理事会组织的考试，目标是获得一张由该协会颁发的"正派黑客证书"。这一证书在业界大大有名，获得广泛认可。尽管学校会专门帮助学生辅导有关考试内容，

但通过考试拿到证书并非人人都能做到，因为证书名称中“正派”两字，才是最具含金量的。

学生之一、在加州州立大学负责网络安全的本·素金就表示:“坦白地说,我知道这证书并非人人都能拿到。如果你不遵守纪律和规定，那么你是不可能通过考核的。”

任务：以黑制黑

黑客学校的最终任务，无疑是让学生通过所学防范黑客，以黑制黑。

据估计，黑客的攻击行为每年给全球带来数十亿美元的损失，为防范黑客攻击而导致的费用也随之不断上涨。一项研究显示,大公司在技术方面的总开支中有 12% 专门用于安全防范，比 5 年前增加了 3 个百分点。“这实在是把利刃，事实上它是如此的锋利，以至于让人感到可怕,”一名业内人士评价说。

在这样的背景下，黑客学校应运而生。一家设在佛罗里达州的学校于 1997 年以 3.5 万美元投资起家，本来是培训微软和思科公司的软件及系统工程师。但在“9·11”事件之后，学校将授课重心放到了信息安全课程培训方面。该校现在每年提供约 200 个培训班，全年收入达 1500 万美元。

“让黑客远离公司网络系统的唯一办法是知道他们在攻击时如何下手,”学校总裁戴夫·考夫曼说,“为此,我们在授课中努力尝试让学生学会知道黑客是如何思考的。”

“乡村天才”与“震荡波”病毒

2004年5月8日，德国警方在汉诺威城附近的村庄瓦芬森拘捕了18岁的高中生斯文·贾斯昌(SVENJASCHAN)。警方指控他涉嫌编写了上周席卷全球的“震荡波”病毒，至少造成了全球1800万台计算机的感染，直接损失高达几百万美元。如果罪名成立，这名德国高中生将为此付出5年监禁的代价！5月10日英国《泰晤士报》和《独立报》对这名德国高中生的人生轨迹进行了跟踪报道。

-“乡村天才”竟是电脑黑客

少年黑客斯文出生在一个做电脑生意的家庭，他母亲开了一家叫“PC帮你忙”的计算机商店。从小的耳濡目染使他非常爱好摆弄计算机，并渐渐上了瘾。

8日，警方突袭了汉诺威附近的村庄瓦芬森。调查人员在他的卧室里发现了一台自己安装的计算机，里面据称包含了“震荡波”病毒的源代码。据悉，这名高中生还没有完成自己的毕业考试，只获得了计算机专业的普通成绩。9日，德国警方开始审问斯文。斯文被警方拘留后不久就获保释，警方正在考虑向他提出计算机破坏罪，这项罪名最终可能导致5年的监禁。这名少年在被捕后立即招了供。他说，“我承认自己低估了破坏的程度。”被捕后，斯文向警方坦白说，他最初的想法只是开发出一种对付“MyDoomandBagle”这类病毒的反病毒，但结果却出现了一种新的“Netsky”蠕虫的变种。这种病毒能够设法让反病毒软件丧失作用，偷盗电子邮件的

地址，自我复制共享网络的文件夹。

邻居们眼中的少年黑客斯文是一位欢快的小伙子。他一头短发，特别痴情足球，他希望今后学数学。他的计算机专业课老师说，“他并没有什么怪异，他只是一名可爱的、有点内向的男孩、好学生。”在晚上，他会像几百万少年一样，把时间都花在计算机屏幕前，认识他的人中几乎没有人把这看得有多么重要。在瓦芬森村大约住着 800 多人，惟一的公共娱乐只是定期到当地一个海边的简陋唱诗班参观。少年黑客斯文据信是受到“打败微软”的刺激后才编写了“震荡波”病毒，他并不是想在全世界故意制造混乱。德国媒体纷纷把这位搅得计算机界一时间天昏地暗的德国高中生称为“乡村天才”。

-25 万美元悬赏让破案没费多少力

调查人员最初怀疑“震荡波”病毒的制造者来自俄罗斯。如果没有任何举报出现，警察至今仍会漫无边际地搜寻罪犯。幸好有微软夸下了海口：保证出资 25 万美元重奖告密者！因此，“震荡波”一案的破获并没有花费多大的力气。如果斯文被判有罪的话，那么举报者还可得到 25 万美元奖赏。

德国警方现在正处于高度戒备之中，他们严密注视着诸如“Kaos 计算机俱乐部”的黑客团伙在这个国家猖獗的活动。这个黑客团伙经常在互联网上交换如何突破计算机安全的窍门。9 日，警方又搜查了另一名“黑客”的家，这名 21 岁的青年住在德国南部，警方怀疑他制造了“PhatBot”病毒。

德国警方认为，18 岁的斯文属于世界最大的黑客团伙的一分子。他与 21 岁的“Phatbot”病毒的编写者都是在上周末被德国警方拘捕的，他们都因与“震荡波”

病毒有联系而落网。

盖茨:微软在安全方面的成就

恶意软件代码已经存在了数十年，但是只在最近几年，由于互联网、高速网络连接和数以百万台新式计算机设备的出现，组成了真正意义上的全球网络，病毒和“蠕虫”才有条件在短短几分钟内肆虐全球。

与此同时，黑客犯罪分子的手法也越来越猖獗，他们制造并散布了诸如 Slammer、Blaster（冲击波）,Sobig（巨无霸、大无极）和 Mydoom（诺维格）等数字病毒，这些病毒像瘟疫一样可以在瞬间大规模扩散，威胁着高科技驱动生产、商务和交流的潜在能量。

病毒攻击的种类也在进化。例如 Blaster（冲击波），这种病毒攻击个人电脑，将无辜的用户在不知不觉的情况下变成了“蠕虫”的传播者。这些攻击方式的特点是：“密集”的攻击互相配合，产生成倍的、排山倒海式的效果，对安全构成了更大的威胁。这就要求 IT 专业人员和消费者提前采取预防性措施，同时也要求技术领域不断革新和开发新的解决方案。

尽管未来充满了各种挑战，但微软乃至整个业界都正在安全方面不断取得重要的进展。本邮件将向您阐述微软在安全的四个领域中所作的重大投入：

- 隔离与恢复
- 更新
- 质量
- 验证与访问控制

此外，我们还承诺在客户教育和合作关系方面加大投入，因为这些将有助于加强计算环境的安全性和可靠性。

因为人的天性，不断演进的威胁模式、越来越多的互联计算机、以及安全恶意利用的数量永远都不会有消失的一天，但是，我们仍然可以显著地防范并减弱网络犯罪所带来的影响。目前，我们正在把研发投入中相当大的一部分用在安全方面。

隔离与恢复

我们安全工作的中心任务是通过将恶意代码隔离来防止恶意代码探索到缺陷，并且提供对计算机程序对话方或协同工作的对象的更加有效的控制，使系统更加容易恢复，这样系统就能够识别并阻止可疑或者恶意的探索行为。

WindowsXPServicePack2

我们正在隔离和恢复措施方面取得很多进展，这些进展将可以帮助我们的重点客户对付操作系统所面临的四种攻击模式。WindowsXPServicePack2 将在今年春夏之交面世。

网络保护

Windows 防火墙将在默认状态下启动，全局防火墙设置以及防火墙中心管理配置也将默认状态下启动。这些措施将减少病毒对个人电脑和网络的“攻击面”。

安全网页浏览

为了减弱恶意代码以及那些会破坏计算机或欺骗用户的网络站点带来的冲击，IE 将自动屏蔽非请求的网站下载以及用户不想要的自动弹出窗口，除非用户点击下载链接。IT 管理员也可以对此功能进行管理，以便在机

构内部保证策略的一致性。此外，无线设置也将得到改进，以加强家庭无线网络浏览的安全性。

安全的电子邮件和即时通讯

为了降低受到攻击的风险，我们正在将OutlookExpress和WindowsMessenger即时通讯的文件附加功能打造得更加出色，此外，在OutlookExpress中增强了用户对外部内容的下载的控制权，那些外部内容的下载会造成邮件发送者识别您的计算机。

内存保护

专门利用缓冲区溢出的恶意软件可以使大量的数据被复制到计算机的内存中。虽然没有单独的技术可以完全消除这种缺陷，但微软正在通过使用大量的安全技术来减弱此类攻击带来的影响。首先，核心的Windows组件都已经使用最新版本的编译技术进行了重新编译以防溢出。微软还正在与Intel和AMD等微处理器厂家合作，帮助Windows支持硬件增强数据执行保护，也就是NX，或“noexecute”。除非某个位置明显含有可执行代码，否则NX通过CPU将应用程序中所有的存储位置都标识成“不执行”。因此，当“蠕虫”或病毒在内存储中标识为“只存数据”的部分插入程序代码时，该代码将无法运行。

WindowsServer2003

由于每台计算机所处的环境都可以被认为是“敌对世界”，因此我们在WindowsServer2003上的工作重点就是探索如何降低、减轻或者抵制威胁。我们计划在2004年的下半年推出WindowsServer2003ServicePack1，其中包含基于服务器的安全增强特性，有一些安全技术始自WindowsXPSP2。为了改进隔离功能，Windows防火墙

将在新服务器安装时就启动，因此服务器可以在配置期间更好地抵御基于网络的攻击。此外，我们还将提供一个安全配置向导，一旦服务器角色（如文件服务器、应用服务器等）启动，就可以根据它们相对应的使用模式锁定服务器的角色。

InternetSecurityandAccelerationServer(ISAServer)2004 版

ISAServer2004 版中的安全功能包含了大量的深度内容检查，使用户可以更好地保护微软应用程序并加强远程 VPN 连接的安全。增强的用户界面和管理工具将使用户更方便地实行和管理安全策略，降低错误配置的可能性，而错误配置正是导致网络被入侵最常见的原因。

Exchange 边界服务

这项新技术主要针对的是出现在互联网邮件中越来越多的安全问题。Exchange 边界服务的设计目的是阻止恶意邮件和垃圾邮件的接收和发送、保护邮件服务器免受攻击、防止邮件携带病毒，以及对信息进行加密以达到最佳安全效果。此外，它还为第三方开发者提供了一个基础，使他们可以开发新一代的邮件过滤器、邮件加密产品以及邮件传递解决方案。

积极的保护技术

阻止和遏制攻击很关键的一点是，保证计算机即使是处在“蠕虫”和病毒越来越复杂的情况下，也更加容易恢复。为了做到这一点，微软正在投资开发一套完整的保护技术，它包括：

动态的系统保护

它可以根据每台计算机“状态”的变化主动调整防御措施。这些状态例如，新软件安装、配置的必要更新，

或者连接到其它网络，那样的话计算机更容易受到攻击。动态的系统保护可以侦测到这些变化并且对保护等级作出相应的调整。现在，客户受益于 Windows 的“自动更新”功能，因为它可以探测到计算机对安全更新的需要。在未来，微软设想的计算机不仅能够侦测到变化，而且能够针对变化主动作出反应。例如，当一台笔记本电脑从公司的网络转移到家庭的电缆调制解调器或 DSL 连接时，它的防火墙就会关闭更多的端口，以提供更多的保护。

行为屏蔽

这种措施可以拦截可疑行为并对其进行判断，如果发现异常就加以阻止，从而限制了计算机受到“蠕虫”或病毒感染的可能性，防止病毒造成更多的破坏。例如，Blaster（冲击波）“蠕虫”就是探索到一个缺陷，导致 Windows 将“蠕虫”复制到其他计算机。而行为屏蔽可以遏制这种攻击。

应用感知防火墙和入侵防御

其目的是识别并屏蔽恶意的传输。隐藏在合法的网络传输中的病毒和“蠕虫”可以绕过传统的防火墙。但这项新的技术将对网络传输进行深层次的检查并阻止或限制恶意内容的扩散。

反垃圾邮件工具：由于病毒、“蠕虫”以及其它恶意代码经常通过垃圾邮件传播，微软正在进行多方面的反垃圾邮件工作。去年 11 月，微软推出了“SmartScreen”技术，这是一种可以用于客户端和在线邮件程序的过滤器。邮件用户可以通过训练过滤器识别垃圾邮件，让它可以变得越来越“聪明”。上个月，微软又发布了 Caller-ID 技术的一个典型应用，它可以对电子邮件的来源进行检

验，类似于电话的来电显示。在法律方面，微软去年在全球范围内对垃圾邮件制造者提起了 66 起法律诉讼。

客户端检查

对于公司来说，最大的一个担忧就是感染了病毒或“蠕虫”的家庭计算机或远程笔记本电脑与公司的网络相连接。我们正在研究的技术可以对远程设备进行检查，如果它们没能通过安全检查就将无法登录到公司网络。

网络服务

2002 年推出的“网络服务安全”（WS-Security）是一项标准化的规范，可以提高网络服务的完整性、安全性和机密性，它允许对信息进行加密并支持数字签名，从而有助于商家以更加安全、经济和灵活的方式连接内部和外部系统。WS-ISecurity 档案工作组最近发布的一项报告介绍了一些新措施，这些措施可以防止在建立共享操作的网络服务中出现的攻击和威胁。

更新

到目前为止，对软件进行更新一直是用户应对安全漏洞的主要方法。日益严重的威胁要求我们采取更加广泛和多样的措施来应对，微软正在继续大幅度地提高更新程序和其它相关程序的质量，并且开发出更加先进的工具来帮助 IT 管理员优化他们的安全基础设施。

去年秋季，为了加强补丁更新程序的可预测性和可管理性，我们开始了按月发布更新程序（当然，在有新威胁出现的情况下我们也会随时推出更新程序来保护客户）。同时，我们也在改进测试程序，争取将更新程序的不一致性和撤回率降到最低。到今年夏季以前，大多数的更新程序都将拥有完全的回滚功能。

去年 11 月发布的 SystemManagementServer2003 是

一种综合的更新程序，也是一种软件管理和分配解决方案，它可以使机构迅速方便地以系统方式部署最新的更新程序。在1月份，我们发布了MicrosoftBaselineSecurityAnalyzerv1.2，这是一种免费的工具，它可以提供识别常见的安全错误配置的最新方法。

WindowsUpdateServices是SoftwareUpdateServices1.0（SUS）的新的发展，也是微软在补丁和更新管理战略中向前迈出的重要一步。作为Windows服务器的免费组件，WindowsUpdateServices赋予了IT管理员权限，使他们能够在Windows服务器和客户端电脑上进行无缝地更新、扫描和安装。新的特色包括向用户提供更多自动操作和控制的权限以减少系统更新时的中断现象，以及扩展功能以SQLServer、ExchangeServer、Office2003和OfficeXP的更新。目前这种服务正处于测试阶段，计划于2004年的下半年发布。此外，对于消费者，我们还正在为WindowsUpdate补充一项新的服务，使消费者可以自动随时获取Windows以及Windows以外的更多的微软产品信息。这项名叫MicrosoftUpdate的新服务将于今年晚些时候推出。

同时，我们还在整合一些功能以实现自动检测关键安全功能的状况（如防火墙、自动更新和反病毒）。在WindowsXP控制面板中提供的新的“安全中心”功能将为用户提供信息，告诉他们关键安全功能是否已经启用以及是否过时。当发现问题时，用户将收到通知和推荐采取的安全措施。

质量

正如我们以前所说，微软坚守自己的承诺，在开发

软件时使用最为先进的设计理念、标准和方法。我们一直严格地实践“设计卓越”的主动性原则，确保我们的工程师在软件设计、开发、测试和发布的过程中理解和采用最佳理念。

去年 WindowsServer2003 发布前我们所进行的安全开发过程就是一个最好的例子，充分说明了我们的努力在一些方面产生了有益于用户的成效。在产品面市后的第一个 320 天中，针对 WindowsServer2003 所发布的“严重”或“重要”的公告数量与 Windows2000Server 相比从 40 下降到了 9。与此相类似，对于 SQLServer2000 而言，在 ServicePack3 发布后的 15 个月中，我们共发布了 3 个公告；而在 ServicePack3 推出前的 15 个月中总共发布过 13 个公告。在 Exchange2000SP3 发布后的 21 个月中，我们只出了 1 次公告，但在发布之前的 21 个月中共有 7 个公告。

我们还在开发新的内部工具方面取得了显著的成就，这些工具可以软件开发时自动对代码进行检测并发现常见错误，还可以在软件发布前对其进行更加彻底的测试。例如，我们使用代码检测工具自动寻找各种可能导致安全缺陷、程序崩溃或中止的问题。我们承诺，将通过培训和工具（包括 VisualStudio 的下一个版本）使其他软件开发商也可以有效地运用我们的技术。

在 WindowsServer2003 的 ServicePack1 中，我们将继续努力，摒弃过时的和未使用的技术，以减少可能遭受表面攻击的区域。

验证与访问控制

计算机网络不再是个封闭的系统，在这个系统中用户只要在网络上就已经提供了识别其身份的依据。在一