计算机百科知识

计算机网络安全

(六)

本书编写组　编

山东科学技术出版社

图书在版编目(CIP)数据

计算机百科知识/本书编写组编．—济南：山东科学技术出版社，2003

ISBN 7-5331-1651-8
Ⅰ．计… Ⅱ．本… Ⅲ．计算机网络—基本知识—汇编
Ⅳ．TP39
中国版本图书馆 CIP 数据核字(2003)第 004271 号

山东科学技术出版社出版发行
(济南市玉函路 16 号 250001)
全国各地新华书店经销 莒县新华印刷厂印刷
开本：787×1092 1/32 印张：240 字数：4 000 千字
2003 年 7 月第 1 版 2003 年 7 月第 1 次印刷
印数：1～1 000 册
书号：ISBN 7-5331-1651-8/D·112
定价：698.00 元

目 录

十月—电脑病毒攻势骤紧

就在大家还在为今年没有什么恶性的病毒感到庆幸的时候，从 10 月 2 日出现的“妖怪”病毒开始，在半个月之内连续出现了包括首例通过MSN进行大规模传播的“佛来芒”病毒(GFLemIng)，通过局域网共享资源进行传播的“新蠕虫”(Opasoft)等几个大规模传播的新型病毒。10 月，人们面临电脑病毒的围攻。

从金山公司公布的 10 月份电脑病毒感染情况来看，目前，上述几例病毒已经在国内广泛地传播，比如，“佛来芒”病毒在短短两三天之内受感染的用户就超过了万人，幸而该病毒对个人用户没有大的直接危害。虽然 10 月份连续出现的重大病毒都没有对电脑用户的计算机产生严重的破坏，但是，由于这些病毒的编写者采用了新的技术，使出现的几个重大病毒具有了新的特点。

据金山公司毒霸事业部技术总监陈飞舟介绍，10 月份出现的病毒具有几个新的特点：

IE 漏洞成为入侵最重要的通道通过 IE 浏览器感染病毒，已经成为目前计算机用户感染病毒比率最高的方式。在今年 9 月公安部进行的 2002 年中国计算机病毒疫情发布会上，国家计算机病毒应急处理中心副主任张健就指出，今年病毒感染类型基本上都是通

过浏览器感染的，这种病毒的用户感染数量非常大，造成很多浏览器的配置被修改，以及磁盘的数据被破坏。而在 10 月最新出现的几例病毒都呈现了利用浏览器和系统的漏洞进行感染和传播的趋势。因此，目前很多反病毒软件都把修补系统漏洞作为自己很重要的一项功能，在国内的反病毒软件中，“金山毒霸”是做的比较早的一个。

即时通讯工具成为攻击对象和传播渠道从“佛来芒”病毒可以看到，由于该病毒通过 MSN 的好友列表进行自动传播，更具有隐蔽性，因此，“佛来芒”病毒的传播速度比预期的要快得多，幸而该病毒对计算机不会造成直接的损害。但是，在即时通讯工具成为病毒传播的主要渠道时，不排除像 CIH 这样的恶性病毒会通过 QQ、ICQ、MSN 等渠道进行广泛传播的可能，因此，加强对即时聊天工具的监控和保护是现在电脑用户的当务之急。

电脑病毒甚至可以自动升级“新蠕虫”病毒就给自己留下了一个后门程序，可以定期从固定网站给自己下载升级包，这样，被感染的计算机实际上已经完全被病毒制造者掌握了，一个破坏使用者电脑的指令可以随时通过“新蠕虫”病毒自动下载并运行，而计算机用户却毫不知情。对来自互联网的各种数据包和

信息的监控和监测变得越来越重要，像“金山网镖”这样的个人网络防火墙也将一改以前不被国内用户所接受的现状，成为和反病毒软件一样的电脑必需品。

陈飞舟同时表示，虽然 10 月份出现了这么多具有新特点的电脑病毒，但是，在国内，目前感染情况最严重、传播最广泛的仍然是今年 4 月份就已经出现的“求职信”病毒，虽然国内各大反病毒软件厂商都早已经解决了该病毒，但现在，金山反病毒应急处理中心监测到每天新感染的用户仍然超过千人。这反应出我国普通计算机用户在反病毒意识和反病毒软件的应用方面仍然需要加强。

反病毒专家：贺卡邮件不是病毒不具危害性

近段时间，许多互联网用户都收到过一封陌生的电子贺卡邮件，怀疑是病毒的行径。目前反病毒专家对此表示，互联网用户需要留意这种看似病毒的垃圾邮件，但最近的贺卡邮件并不是病毒，实际上是贺卡公司的一种网上营销活动。反病毒公司一再强调，收到这种贺卡邮件的用户，其机器并没有被感染，它不是什么病毒或蠕虫，用户尽管放心。

据悉，这种大量传播的邮件会让用户从 FRIend GReetIngs.com 站点上浏览电子贺卡，而当用户从该

站点打开贺卡时会自动安装一软件到用户的机器上。若用户接受其注册协议，程序就会自动将贺卡再发送给地址簿中的所有联系人。而通常用户不会去阅读协议，直接接受，这就导致大量的令人感到厌烦的邮件被发送出去。

国外著名反病毒公司 Sophos 的高级技术顾问 GRahamCLuLey 指出，是否想在自己机器上安装某个程序是每个用户自己决定的事，不过用户在安装任何程序之前都要仔细辩阅读条款和协议。目前的贺卡程序只是一种令人厌烦的东西，它会产生大量垃圾邮件。

WIFI 将提高无线局域网安全性

无线以太网兼容性联盟（WECA）周二宣布推出一系列机制，试图克服阻碍无线网发展的安全问题。WECA 保证带有 WIFI 标签的无线局域网产品符合 IEEE802.11 标准。

WECA 一位官员透露，WECA 打算用新的标准取代目前的基于 WEP（无线加密协议）的安全系统，但没有提供更详细的细节情况。

WEP 内置在使用 IEEE802.11b 和 802.11a 标准的产品中。攻击者很容易侵入 WEP 系统。IEEE 中负责 801.11 标准的一个小组目前正在开发一个新的安全规范，要求设备支持集中不同类型的功能更为强大的

算法。目前这个工作还在进行中，到明年下半年之前，不会有采用新标准的产品问世。

分析人士指出，安全问题关系到人们对无线局域网的接受程度，特别是企业用户更关心无线网络的安全性。

一些厂商（比如 CIsco 公司）销售的产品中包含采用 802.11 标准的安全系统，同时也包含建立在 WEP 之上的其他安全保护系统。但是，大多数面向普通消费者的无线局域网设备仅仅提供基于 WEP 的安全系统。

1/3 的网络瘫痪由人为失误引起

据日经BP社报道，“企业和机构的网络瘫痪故障，有 1/3 是由于人为失误造成的”——从事网络结构控制设备业务的美国 GoLdWIReTechnoLogy 于美国当地时间 10 月 28 日，引用美国调查公司 YankeeGRoup 的调查结果发表了上述观点。

此次调查是 YankeeGRoup 于 2002 年 8 月以北美的企业及政府机构的网管为对象进行的。共有 229 人参与此次问卷调查。

调查显示，35%的网络瘫痪故障是由于通信运营商或 ISP（互联网服务提供商）造成的。排在第二位的是起因于人为失误，其比例占 31%。此外电源故障

占 14%，硬件故障占 12%。另外“问题未得到解决，原因不明”的故障占 8%。

人为失误的主要原因是“交换机、路由器和防火墙等通信设备的配置控制不够充分”(YankeeGRoup)。在企业和机构中，绝大多数事故是由于未经授权的人随意改变了设备配置。调查另外还显示，在过去一年间有半数左右的企业和机构出现过这种故障。

“尽管因行业不同情况各异，但如果网络瘫痪一个小时，将会造成 9 万--450 万美元的损失。此次调查表明，最大可将故障发生减少 30%。只需努力做到‘排除人为失误’，就能够大幅增加网络运行时间(UptIme)”(YankeeGRoup 副总裁 ZeusKeRRavaLa)，解决方法是“制定若干条简单而行之有效的基本操作规程”。

此次调查结果的概要如下：

31%的网络瘫痪故障因人为失误而起；

其中 83%都与网络运行上所必须的设置变更作业无关；

70%的企业和机构使用通用密码；

68%的回答者对登录信息和配置变更无法进行跟踪了解

Windows、Linux 是受到攻击最多操作系统

技术风险管理公司 mI2g 在一份报告中指出，苹果公司的操作系统 MacOS 是 2002 年受黑客、蠕虫、病毒攻击最少的操作系统之一，微软公司的 Windows 和 Linux 是受到攻击最多的操作系统。

mI2g 公司表示，在 2002 年的头 10 个月中，共发现了 1162 个软件缺陷，其中包括在操作系统、服务器软件和第三方应用程序中发现的安全缺陷。在这些缺陷中，与 MacOS 有关的还不到 25 个。安全缺陷与 MacOS 同样少于 25 个的还有康柏公司的 TRu64 和 SCO 集团公司的 SCOUnIx。与此形成鲜明对比的是，攻击微软公司的 Windows 操作系统的缺陷有 500 多个，攻击 Linux 操作系统的缺陷有 200 多个。

尽管今年头 10 个月发现的缺陷数量低于去年全年发现的 1506 个缺陷，但 mI2g 公司指出，发现缺陷的速度正在增加，10 月份发现了 301 个缺陷。

报告还发现，2002 年是数字化攻击最严重的一年，头 10 个月发生的攻击数量已经高达 58000 次，比创记录的 2001 年的 31322 次还高出了 54%。

mI2g 公司发现，与市场份额相比，操作系统中被发现的缺陷数量与操作系统被攻击的可能有更大的关系。MacOS 的市场份额在 3%5%之间，只是 31 次攻击的目标，占所有攻击数量的 0.05%。微软公司的

Windows 的市场份额超过了 90%，占攻击总数的 54%。

据 mI2g 公司称，这些攻击给全球带来的损失高达 73 亿美元，如果考虑蠕虫、病毒等所谓的“隐形”攻击，这一数字可能会增加到 330 亿 400 亿美元。

加强政府机构 IT 安全 NIST 发布安全指南草案

美国政府发布了帮助政府非军事机构确保不受互联网攻击和内部攻击的三个文件之中的一个文件。

美国国家标准与技术研究所（NIST）本星期发布了第一个标准草案。这个文件将帮助政府非军事机构制定衡量系统安全的标准。最后定稿以后，这个标准将允许机构说明它们的系统可以提供的安全等级。这个等级在联邦机构之间共享数据的时候是非常重要的。

据介绍，这个标准解决了如何衡量网络风险或者雇员非法进入应用程序、软件或计算机网络的问题。联邦机构的高级官员要在考虑的威胁和安全漏洞的前提下批准使用计算机系统。由于总是会出现一些遗漏的风险，因此机构的高级官员要判定这种威胁是否可以容忍。

这个文件告诉信息系统管理人员如何在系统保密、保持完整性以及保持运行和可用性等方面为他们

的网络和应用程序评级。

据这篇报告称，从 2002 年 3 月开始，这个计划就在为保证和鉴定联邦信息系统制定标准指南。这个计划还要确认联邦信息系统可以接受的最低安全标准，促进公共和私营评估实验室的发展以及个人的安全认证。

这个标准文件是三个文件中的的一个，主要介绍机构如何保护自己免受网络和内部人员对其计算机系统的攻击。第二个文件将在 2003 年春季发布，将主要介绍每个联邦机构必须保证的最低安全标准。第三个文件也将同时发布，告诉审计人员如何查对已经妥善保管的计算机系统。

目前这个文件的草稿名称是《IT 系统安全认证与鉴定指南》，将在 2003 年 1 月 31 日之前公开接受公众的评论。

微软新发现 Windows 一处“危险”级漏洞

微软公司 30 日警告称，执行虚拟个人网络中一个协议的软件代码中存在的瑕疵使 Windows2000 和 WindowsXP 系统易受到拒绝服务攻击。

微软公司在其第 MS02063 号安全公告中称，执行 PPTP 协议的代码中存在未经检查的缓冲漏洞，该协议使用户建立并使用虚拟个人网络，Windows2000 和

WindowsXP 系统均支持该网络。

微软公司认定该问题属于“危险”级。（详情见 http://www.Microsoft.com/technet/Security/Bulletin/MS02063.asp）

PPTP 协议是 Windows2000 和 WindowsXP 服务器版本中路由和远程访问服务中的一个选项，也是工作站版本中远程访问客户机的一部分。

微软公司称，只有开启了 PPTP 协议的系统才处于危险之中。

微软公司称，尽管由于客户机每次建立连接是一般改变其 IP 地址，从而使攻击客户机非常困难，但服务器和客户机均处于危险之中，微软公司称，攻击者可通过向系统发送错误格式的 PPTP 协议控制数据而使一个脆弱的系统崩溃。

一个可修复该问题的补丁程序现可在微软公司 TechNet 网站上下载。

微软公司称，提供 PPTP 协议服务的系统管理员必须立即进行安装，使用 PPTP 协议进行远程访问的用户也应考虑安装这个补丁程序。

微软公司 30 日发布的另一份安全公告中还就另一个影响 Windows2000 系统的“中等”安全问题发出了警告。详情见

http://www.Microsoft.com/technet/Security/Bulletin/MS02064.asp

该软件的默认许可设置可使“每一位”用户拥有完全访问系统根文件夹的权限。

微软公司称，通过在根目录中放置一个程序，并让它在另一位用户登陆时运行，攻击者可对同一系统的用户发动特洛伊木马攻击。

微软公司称，系统管理员应考虑修改Windows2000根目录的访问许可。

新款OutLook软件将具防范垃圾邮件功能

微软公司的下一代OutLook电子邮件和通信录管理软件将会更加认真地对待垃圾邮件问题。

在预览网页格式的邮件时，OutLook11的默认设置将不再从外部服务器下载图片等数据。

可以收发HTML格式的邮件曾一度是微软公司的OutLook电子邮件程序的与众不同之处。

OfficeXP产品经理SImonMaRks上周表示：“可以说我们倒退了一步，当你预览邮件的时候我们阻止外来内容的进入。”

MaRks把这种新的功能描述为一种重要的反垃圾邮件工具。

HTML格式的邮件所包含的图像、声音和视频等数

据通常都是从一个 Web 服务器下载而来的，OutLook 预览时下载这些内容的方法与Web浏览器下载数据的方法非常相似。

但在通过 Web 浏览器获取内容时，人们通常是决定要去那个网站看看。

基于Web的垃圾邮件有时会给用户发来一些无用的内容，有时还附带有一些小程序。

垃圾邮件始作俑者要想知道一个电子邮件帐户是否被实际使用，他们的伎俩是，如果垃圾邮件中的内容被下载，邮件中一种被称为“Webbeacon”的小程序就会告诉发件人该电子邮件帐户实际上存在。

分析人士说，仅通过预览窗口查看这种垃圾邮件也会激活 Webbeacon。

这个小程序会导致原来的发件人给用户发送更多的垃圾邮件，而且其他使用同一个邮件名单的垃圾邮件传播者也可能会给用户发来一些他们所不想收到的信息。

微软公司过去在保护隐私和增强安全性方面一直做的不够，为了给予这个问题更多的重视，它推出了一系列计划，而这次为 OutLook 推出的新功能就是这一系列计划中的一部分。

FBI 查互联网心脏被黑案称攻击来自美韩

美国联邦调查局(FBI)局长罗伯特穆勒日前透露，10 月 21 日黑客曾对美国 13 台互联网域名系统(DNS)主服务器发动攻击，据查其使用的电脑位于美国和韩国境内。

穆勒是在弗吉尼亚州佛斯彻奇召开的会议上公布这一调查结果的，但他没有具体说明 FBI 目前得到了什么信息，只是称调查仍在进行当中。

这次分散服务拒绝(DDOS)黑客攻击事件发生后，负责管理“A”、“J”两类主服务器的 VeRISIgn 公司发言人称，受到攻击的 13 台主服务器同时遇到使用互联网控制协议(ICMP)信息严重堵塞现象，该类信息的网上发送量短时间内激增到平时的 10 倍。

受到攻击的 13 台主服务器当中，大约有 2/3 的服务器无法向合法用户提供正常服务，用户的服务请求暂时不能满足或服务效率严重下降。

不过，受黑客攻击期间，仍有四五台主服务器始终保持在线状态，使用这些服务器的大部分用户并没有受到任何干扰。

和美国一样，韩国也是出现黑客攻击事件次数较多的一个国家，因为其电脑用户数量庞大，而且韩国电脑用户普遍使用 DSL 或有线调制解调器等宽带接入

方式。

“怪物”取代 KLezH 成为传播最广泛的病毒

据反病毒厂商 Sophos 公司于当地时间 10 月 31 日公布的统计资料显示，“怪物”（BugbeaR）蠕虫病毒的一种变形病毒——BugbeaRA 是十月份传播最广泛的病毒。它取代了上个月的 KLezH，位居病毒排行榜榜首。KLezH 已经屈辰第二位。

Sophos 反病毒中心的反病毒顾问娜塔莎表示，在连续 7 个月高居病毒榜榜首后，KLezH 终于被“怪物”蠕虫病毒从榜首位置顶替下来。“怪物”蠕虫病毒不仅能够通过电子邮件和网络共享进行传播，而且还能够记录被感染的计算机的击键操作，使黑客能够监测用户输入的从口令到银行帐户等在内的所有资料。

“怪物”蠕虫病毒利用了 OutLook、OutLookExpress 电子邮件客户端软件以及 IE 浏览器中的安全缺陷进行传播。

Sophos 公司在 10 月份共发现了 824 种新的病毒、蠕虫和特洛伊木马等恶意软件。

美西部银行泄漏数千客户电子邮件地址

美国东部时间 11 月 5 日(北京时间 11 月 6 日)消息，美国西部银行在业务运营过程中出现失误，泄漏

了数千名客户的电子邮件地址，该银行将这一失误归为“人为错误”。

西部银行的一名发言人称，在发送一份关于银行将于本周末因维修而暂停服务的邮件通知时，西部银行将 3000 多名客户的电子邮件地址全部加到了“发送至”一栏中，而不是“暗送”一栏，这完全属于无意的人为错误。

西部银行当天向受到影响的客户发送了道歉邮件，邮件中说：“我们非常抱歉由于人为错误将您的邮件地址泄漏了出去，我们已经采取了必要的措施保证此类事件不再发生，并对因此可能给您造成的不便致以深深的歉意。”

近年来，由于垃圾邮件对邮箱用户的麻烦引起了各界的关注，因此电子邮件地址越发成为了用户的稳私信息之一。虽然很多垃圾邮件发送者可以购买到内有大量邮件地址的 CD，但那些一般都是些不存在的或无用的地址。

相反，那些象西部银行客户地址这样的真实而可靠的邮件地址就显得非常有价值了。

反垃圾邮件协调小组成立

为保护我国电子邮件服务供应商和互联网用户的正当利益，公平的使用国际互联网资源，同时规范

我国电子邮件服务秩序，由中国互联网协会、263 网络集团和新浪共同发起，另互联网协会反垃圾邮件协调小组近日在北京成立，国内 20 多家邮件服务商首批参加了反垃圾邮件协调小组。

其主要任务是致力于倡导电子邮件服务提供商及全体网民共同行动起来，发对发送、转发垃圾邮件，建立完善反垃圾邮件机制，展开国际上有关组织的交流与合作，共同抵制垃圾邮件。

报告显示：零售及休闲行业的病毒感染率最高

日前有安全报告显示：全球企业及个人面临感染计算机病毒的危险中，从事零售及休闲行业的公司感染率要高于其他行业的企业。

据英国邮件管理安全公司 MessageLabs 的最新报告显示，全球各大行业中，零售及休闲行业的企业中毒率要高于其他行业，平均每 50 封邮件中有一封被病毒感染。与此相比，从事会计审计及法律业务的单位中毒率最低，每 350 封被感染一封。

MessageLabs 公司表示，零售及休闲行业感染率之所以高，是由于这些公司必须与家庭用户保持密切联系，而家庭用户则是最缺乏安全意识的一族，因而成为传播病毒之源。

报告同时指出，金融及银行机构尽管也必须与客

户“亲密接触”，但其感染率也很低，大约 101：1。个中原因在于金融机构对安全非常重视。而 IT 与电信部门的中毒率大约为 162：1。

报告还显示，目前“怪物”（BugbeaR）病毒最为流行，每 324 封邮件有一封被其感染，而 KLez.H 及 Yaha.E 分列二、三名，分别为 479：1 及 1069：1。

国际专家谈网络安全用户认识有三大误区

网络安全被空前重视

在美国，网络安全最近被提到了前所未有的重视高度。美国联邦调查局所属的关键性基础设施保护中心发布了一份题为《关于网络空间安全的国家战略》的报告，第一次明确地将网络安全提升到了关系国家安全的战略高度，第一次将网络安全综合进了关于国家安全的总体思路之中。

该报告指出：“网络空间对于本土安全与国家安全来说都是至关重要的。安全而且可靠的网络空间是支撑国民经济、关键性基础设施以及国防的支柱。因此，‘关于网络空间的国家战略’是一项必须加以实施的战略。”

网络安全的话题现在确实很热。但是，为什么政府和企业不断增加投入，却得不到渴望的安全感？网络安全究竟是什么？一些国际网络安全专家认为，在

目前网络安全热的背后，许多人对网络安全的认识其实还处于初级阶段，并不成熟。

9 月 14 日至 20 日，全球互联网技术标准化组织 IETF 中的 IP 安全协议工作组联合主席芭芭拉福瑞舍(BaRbaRaFRaseR)女士一行来到中国，与国内大型企业和金融业的信息化主管进行了为期一周的“思科安全专家中国行”交流活动。这次活动是由思科公司组织的，作为全球领先的网络公司，思科在 10 多年中确立了自己在信息安全行业中不可撼动的领导地位。思科希望借此行深入地了解中国企业在相关方面遇到的实际问题、潜在困惑和迫切的需求。

用户认识有三大误区

福瑞舍女士说，由于安全专业知识的匮乏和认识上的偏差，对网络安全抱有“投资一次、享受终身”思想的人不在少数，它们大多把网络安全产品和方案理解成一道坚固的静态防线，而不能根据用户网络应用及其拓扑结构的发展变化调整或者重新部署网络系统的安全策略，从而埋下了系统安全的隐患。

归纳起来，国内网络用户在选购网络安全产品和部署网络安全系统的实践中还存在着如下一些认识上的误区：

1.认为没有必要制订符合企业长远发展的安全

策略；

2.面对不法分子日益猖獗的复合式攻击，不少网络用户试图通过单点产品的简单堆砌来加以应对，而对产品之间的协调工作考虑较少，导致了安全防护体系的整体防御能力低下；

3.对复杂多变的网络环境和层出不穷的安全漏洞认识不足，许多用户把已经部署了的安全防御体系看成是“完美工事”。

福瑞舍女士说，思科在全球参与了很多各种企业的网络架构的设计和搭建工作，之所以可以在全球被广泛接受、认可，很重要的一个原因是思科视安全为网络体系不可分割的一部分。思科不仅在网络产品中慎重的加入了一些安全防护的措施；并且在设计网络结构时就对网络需求进行了模块化的分析，以部署适合企业现状而且可扩展的安全防护手段。这样，使得原本不可预期的网络危机转变为可预防、可控制，并且有补救方案的安全防护问题，从而大大降低了企业网络应用的风险。

安全无大小

不难想像，缺乏防卫能力的网络用户正好给不法分子提供了可乘之机，它们顺藤摸瓜地对用户的网络系统发起攻击，于是一道道安全屏障被穿破，一座座

防御工事被摧毁，当然，遭受损失的不仅仅是拥有和使用网络的人们。

福瑞舍女士说，网络安全不分大小，家庭、小企业也应担负起网络安全的相应责任。安全战略的实施应在五个层面上展开：即家庭、企业、关键性机构、国家，以及全体人类。把家庭和小企业用户首次纳入国家信息基础设施安全的范畴之内，这也是《关于网络空间安全的国家战略》这份报告一个很突出的特点。因为由于技术的发展，家庭和小企业中的计算机和网络很容易被犯罪分子单独利用或者集体利用来进攻更大的目标。

把受害 PC 当攻击平台 Roron 蠕虫危害极大

俄罗斯一家杀毒公司 KaspeRsky 实验室 11 月 6 日称，一种新的病毒可能会帮助黑客获得对家庭计算机的控制。但是，其它安全公司却认为威胁没有那样严重。KaspeRsky 实验室把这种新的病毒或蠕虫取名为“Roron”，其它一些公司把它称作“ORor.B”。KaspeRsky 实验室发言人 DenIsZemkIn 说，这种新的病毒可通过电子邮件信息、共享硬盘和 Kazaa 文件共享网络等途径传播。

ZemkIn 说，我们认为，这种蠕虫对家庭用户特别危险。企业用户已经知道电子邮件附件的危险性，可

能不会打开包含这种程序的文件。

KaspeRsky 实验室对“Roron ”蠕虫发出安全警告，因为这种蠕虫的传播途径很多，因此把它列为“高危险 ”等级。这家安全公司还说，这种蠕虫的目的是把受害者的计算机当成发起攻击的平台。每一份病毒文件中都包含几种黑客工具，这些工具让受感染的计算机接受互联网中继聊天室发出的信息的控制。用互联网中继聊天室发出信息，网络破坏分子就可以实施拒绝服务攻击。

然而，赛门铁克公司表示，它最大的可能是把“Roron ”蠕虫列为 5 级危险等级中的第 2 级。赛门铁克公司安全反应小组高级经理 ShaRonRuckman 说：“我们在美国还没有收到有关这种蠕虫的报告。”他补充说，该公司欧洲的客户只收到了几份这样的病毒文件。

KaspeRsky 实验室的客户主要在欧洲，主要集中在前苏联的一些国家。

“Roron ”病毒是 8 月份出现的多数公司都称作“ORor ”的一种电子邮件蠕虫的最新的5个变种之一。KaspeRsky 实验室认为，“Roron ”病毒是在保加利亚制作的，因为这个病毒代码中的一些字是用保加利亚语写的。

台湾通过法律修正草案刑罚电脑“黑客”

据新华社台北 11 月 6 日电设计电脑病毒程序、对外散播造成公众或他人受损害者，在台湾将被处 7 年以下有期徒刑、拘役或 50 万元新台币以下罚款。

台湾有关当局今天通过一项法律的修正草案，针对无故入侵他人电脑、干扰电脑系统、制作专供电脑犯罪程序、妨害电脑使用等罪，增加了多项条文。该草案也针对电脑“黑客”增加了相关规定，无故入侵他人电脑或相关设备，包括输入他人帐号密码、破解使用电脑

保护措施或利用电脑系统漏洞，将被处 3 年以下有期徒刑、拘役或 10 万元新台币以下罚款。

无故取得、删除或变更他人电脑或相关设备电磁纪录，导致公众或他人受损害者，处以 5 年以下有期徒刑、拘役或 20 万元新台币以下罚款。以电脑程序或其他电磁方式干扰他人电脑或相关设备，给公众或他人造成损失者，处 3 年以下有期徒刑、拘役或 10 万元新台币以下罚款。

为防止网络攻击美国互联网根服务器被搬迁

国外网站消息，由于前段时间互联网核心服务器遭至黑客攻击，为安全起见，避免互联网根服务器再次受到攻击，管理两台根服务器的美国 VeRIsIgn 公

司已将其中一台进行搬迁。

据 VeRIsIgn 公司发言人谢丽尔里根周三称，本周二晚上他们将两台根服务器中的一台转移到维吉尼亚北部一个未透露地址的大厦里，并且位于网络的不同部分。此次搬迁的目的是确保硬件损坏或网络遭受攻击时不至影响两台服务器。上一次大规模的搬迁是在 1997 年，当时将 13 台根服务器都进行了转移。

对于 10 月 21 日 13 台服务器中 9 台遭到不寻常的网络攻击事件，FBI 目前发现攻击源自美国及韩国。被攻击的 9 台服务器，当时有 7 台不能响应正常的网络流量，2 台暂时中断。攻击持续了一小时。一小时之后突然停止，管理人员进行一些处理后，服务即得到恢复。VeRIsIgn 公司表示，他们管理的这两台服务器尽管位于同一网络，但在此次攻击中并未受到影响。大部分的互联网用户当时没有意识到攻击，是因为互联网当初的构造就是本着承受短暂中断的目的来构建的。

不过，许多专家仍对黑客成功攻击表示惊讶。在这次拒绝服务攻击中，黑客按照传统方法，通过控制某大学、公司甚至家庭用户的第三方电脑，让他们向目标服务器发送大量数据流。FBI 追踪调查后发现，攻击来源于美国及韩国。

万台电脑运行 549 天成功破解超级密码

想知道破解无线加密软件开发商 CeRtIcom 公司开发的一个密码需要费多大的劲吗？1 万台计算机无间歇运行了 549 天，外加一位数学家的脑力，共同完成了世界最大的单个数学计算之一。

CeRtIcom 公司向科学家、数学家、译解密码高手和黑客提出挑战，请他们破解该公司用于保护数字数据的一个密码。

据圣母玛利亚大学数学研究员兼教师 ChRIs MonIco 称，10 月 15 日下午 12 时 56 分破解成功。他将获得 1 万美元奖金，不过更多的是赢得了荣誉。

CeRtIcom 公司创始人、本次竞赛的发起者 ScottVanstone 说："我们的技术是基于一道非常难解的数学题，因此我们特别希望验证一下它到底有多难。当有人问'有没有黑客试图侵入你们的系统？'我们回答，当然有。事实上，我们鼓励这么做。尽请尝试。现在终于有结果了。"

Vanstone 指出，为破解本次挑战赛的密码所采用的强大计算机功率可以在数秒内破解德国二战期间使用的 EnIgma 密码。

他补充道，这种破解办法只允许一个人的密匙或身份访问，破解的只是 109 位密匙，而 CeRtIcom 公

司保护数据所用的产品则从 163 位密匙开始。

CeRtIcom 挑战赛始于 1997 年，已吸引 247 个小组参加，组员数量超过 1 万，包括译解密码高手、计算机科学家和数学家。

10 月份携带病毒邮件暴涨 42%垃圾邮件减少

据提供电子邮件过滤服务的 MessageLabs 公司最近的研究，今年 10 月份与 1 月份相比，携带病毒的电子邮件数量增长了 42%，平均 134.5 封电子邮件中就有一封电子邮件携带病毒。

MesageLabs 公司扫描了 2.12 亿封电子邮件，其中 1,500 万封电子邮件中发现有潜在的有害内容。在休闲、体育和娱乐行业工作的用户收到了带病毒的电子邮件或垃圾邮件的数量最多，因为这些行业的人与家庭用户关系最密切。病毒邮件针对 IT 行业和通信行业的数量很少。

BugbeaR 和 KLez.h 是最流行的电子邮件病毒，其次是 Yaha.E 和 SIRCam 病毒。10 月份的垃圾电子邮件的比例是 6.1 封电子邮件中有 1 封垃圾邮件，比 9 月份的 6 封电子邮件中就有 1 封垃圾邮件稍有减少。

淫秽垃圾邮件 10 月份比 1 月份有所下降。10 月份每 3,418 封电子邮件中有一封含有淫秽图像，自从 1 月份以来这个数字下降了 23%。

赛门铁克软件有瑕疵诺顿 2003 遭投诉

美国当地时间 11 月 8 日消息，赛门铁克公司 11 月 8 日称，它已经修复了“诺顿网络安全特警 2003”(NortonInternetSecurity2003)套装软件中的一个瑕疵。这个软件瑕疵能使电子邮件到达用户邮箱之前被删除。已经有部分用户投诉说，“诺顿网络安全特警 2003”正在删除电子邮件。赛门铁克公司在英国的发言人 KatheRIneJames 说，对于被删除的电子邮件，用户收件箱都会出现一条信息，主题是“赛门铁克电子邮件代理删除的信息”。

James 表示，“诺顿网络安全特警 2003”软件的一小部分用户曾报告说，他们的电子邮件被意外地删除了。这个事情第一次是在 10 月 14 日发生的。赛门铁克公司本星期发布了一个软件补丁修复了这个瑕疵。这个补丁可通过该软件的在线更新功能下载。

“诺顿网络安全特警 2003”套装软件包括防病毒、防火墙、隐私控制、垃圾邮件报警等软件。这个软件瑕疵出现在反垃圾邮件那部分软件中。反垃圾邮件功能是要过滤掉发往用户邮箱的任何不需要的商业电子邮件。

James 说，如果用户连续使用计算机并且收到大量的电子邮件，或者用户已经把电子邮件客户端软件

设置成经常检查邮件服务器，诺顿反垃圾邮件预警软件可能会引起内存分配错误，造成电子邮件被删除。

赛门铁克公司认为，由于投诉的人数不多，因此，受这种软件瑕疵影响的用户只是一少部分人。不过，赛门铁克公司没有说，有多少用户提出了投诉，以及这些用户都在哪里。“诺顿网络安全特警 2003”软件目前在世界各地都有销售。

James 表示，用户可使用该应用程序中的在线更新功能下载补丁程序，修复这个内存分配错误的软件瑕疵。病毒警告竟带蠕虫安全公司遭黑客冒名

11 月 8 日，俄罗斯杀毒软件公司 KaspeRskyLabs 向用户道歉说，一封发出病毒警告的电子邮件感染了它在警告信息中说的那种蠕虫。

KaspeRskyLabs 公司称，该公司向用户发出的“病毒新闻”电子邮件实际上是黑客假冒该公司的名义发出的。这些黑客突破了该公司在莫斯科的计算机系统，窃取了订阅这个新闻的用户的电子邮件列表。

这家公司的创始人和研究负责人 EugeneKaspeRsky 说：“我们正在进行调查以披露这次攻击的起源……并且保证将来不让这种攻击得逞。”

到目前为止，KaspeRskyLabs 公司还没有接到任何因接到这个邮件而受到病毒感染的投诉，但是，该

公司表示愿意为任何受到这种病毒感染的用户提供免费的服务。

这种受病毒感染的电子邮件已经发给了 1000 多个用户，电子邮件携带的病毒是最近发现的“BRaId”蠕虫。

KaspeRskyLabs 公司把“BRaId”蠕虫也称作“BRIdex”。这种蠕虫传播的范围不广。英国电子邮件服务提供商 MessageLabs 在过去的 24 小时里为客户公司拦截了 2000 封含有这种病毒的电子邮件。这种病毒在 MessageLab 公司的每日前 10 位恶意程序排行榜中排在第五位。KLez 病毒排在第一位，在过去的 24 小时里，该公司拦截了 9000 封包含这种病毒的电子邮件。

Windows 安全性被质疑微软对此有话要说

微软公司对英国安全情报公司 MI2g 上周发布的一篇报告作出了正式反应。在这篇报告中，MI2g 称，苹果公司的 MacIntosh 和各种 UnIx 操作系统的变体是最安全的操作系统，而 Windows、Linux 是最不安全的操作系统。在 2002 年头 10 个月发现的软件缺陷中，44%与 Windows 有关，19%与 Linux 有关。

在接受采访时，微软公司安全业务部门的副总裁迈克表示，他相信这些数字是误导性的。MI2g 提供的

数字包含了由厂商和用户新发现的缺陷，我们无法确定同一个缺陷是否会被多次统计，以及是否有误报的缺陷。

迈克说，在目前的这种体系下，用户越多的产品，例如Windows，被发现的安全缺陷肯定会越多。但MI2g公司的安德森说，MacIntosh操作系统较小的用户数量不完全是他们得出这一结论的原因。MacIntosh操作系统的市场份额为3%，但这些系统被攻击次数的比例只占0.05%。

在一份声明中，MI2g公司表示，它正在就这一问题与微软公司的高层进行接触，二家公司正在解决安全缺陷的计数问题。该公司的CEO马太表示，即使是不计算“未经证实的”缺陷报告，微软公司的处境也不会好转。与 Windows 相关的安全缺陷的比例将由44%上升到54%。马太说，他们的数字与CERT等专门记录软件安全缺陷的机构基本上相符合的。

软件产业分析家和安全专家认为，考察安全缺陷的数量不是一种能够准确地反映操作系统安全性的方法。

IDC负责系统软件分析的副总裁库斯耐兹基说，比较软件中的安全缺陷数量是有趣的，但用处不大。重要的是软件厂商对发现的安全缺陷的反应速度。

eEye 数字安全公司的黑客事务总监迈弗里持相同的看法。

库斯耐兹基和迈弗里都表示，尽管苹果公司的操作系统中的安全缺陷数量较少，但黑客对它不感兴趣是它的攻击次数少的主要原因。攻击苹果计算机给黑客带来的成就感远不能和攻击 PC 相比。用户在选择操作系统时更应当关注确保系统的安全和厂商对安全缺陷的反应速度，而不是操作系统中安全缺陷的数量。他们二人还对微软公司在安全性方面的表现提出了批评。

《电脑报》：行动起来反垃圾邮件

2002 年 11 月 1 日，中国互联网协会、263 网络集团和新浪等单位共同发起的中国互联网协会反垃圾邮件协调小组在北京正式成立。中国互联网协会希望通过这个协调小组联合业界各公司从理论、技术和个人行为等方面进行深入、有效的协商和探讨，共同制定和实施反垃圾邮件的相关措施。

垃圾邮件泛滥成灾

中国互联网协会把以下这些邮件定义为垃圾邮件：1.邮件人事先没有提出要求或者同意接受的广告、电子刊物、各种形式的宣传品等宣传性的电子邮件；2.收件人无法拒收的电子邮件；3.隐藏发件人身

份、地址、标题等信息的电子邮件；4.含有虚假的信息源、发件人、路由等信息的电子邮件。这些邮件的产生是因为一些人看到利用网络发送宣传邮件成本低、速度快，是一个很好的“宣传途径”。由于垃圾邮件无休无止和源源不断，让人防不胜防，有些人听之任之，有些人已深受其苦。

新浪网的首席技术官严援朝先生说，垃圾邮件的危害越来越严重，我们现在是在进行追逐似抵抗。极端分子就曾连续一个月对新浪发送大量垃圾邮件攻击网站，迫使新浪的技术人员一个小时改变一次应对措施，这是一场非常艰苦的战斗。万网的总经理张向东说，他们公司的员工每天至少要收到100多封邮件，其中 60%都是垃圾邮件。“应该像清理街头小广告一样，对垃圾邮件进行清理，让发送垃圾邮件的人得到惩罚。”

互联网协会副秘书长黄澄清先生说，垃圾邮件不仅消耗网络带宽，而且浪费用户的存储空间。据介绍，根据市调公司的调查资料，企业网络中有36%的邮件是垃圾邮件，这个数据比去年同期增长了8%；有权威人士预计，以一家1万名员工的公司为例，内部产生的垃圾邮件足以使公司损失相当于1300万美元的生产力。

严援朝举例说，互联网基础设施的飞速发展给垃圾邮件的产生创造了条件。比如通过住宅小区的宽带，一栋楼里 10 个家庭的小孩通过 100Mbps 的带宽同时发送就可产生 1Gbps 的发送能力，这个威力不可小视。

反击垃圾邮件

由于垃圾邮件泛滥，今年 3 月以来，由于中国一些 IP 地址发出大量的垃圾邮件，致使中国电子邮件面临被欧美全面封杀的境地。全球大约有数万家公司、组织或者私人网络全面封锁中国的 IP 地址，在被宣布拒绝接受的电子邮件网站名单中，新浪、网易、搜狐、163 邮局、263、21cn 等国内主要邮件服务商赫然在列。

这不仅给正常的交流带来困难，更多的是贻误商机，这也可以看作是垃圾邮件给中国国内用户带来的最直接的最重大的影响。

美国在 2000 年就通过了《反垃圾邮件法案》来对抗垃圾邮件，对于那些违反该法案的发件人，联邦贸易委员会将有权采取行动。网络服务商也可以向联邦法庭提出诉讼，要求违反《反垃圾邮件法案》的人每封邮件赔偿 500 到 50000 美元。

国内也有部分公司已先行行动起来对付垃圾邮

件。在 2000 年，中国电信就规定：因某些用户发送垃圾邮件等不正当使用网络行为影响到其它用户或通信网络正常运行，中国电信有权在不通知用户的情况下，采取对用户进行警告、暂时关闭直至永久停止对该用户服务的措施。在某些用户滥发垃圾邮件对网络通信产生严重影响时，中国电信各级部门将及时向当地执法部门报告并追究其法律责任。

263 网络集团在 2000 年推出了 SMTP 认证，防止垃圾邮件的发送。并且不断在技术上升级、管理上强化，将技术和管理有效地结合起来。

但是这些反垃圾邮件的行动是孤立的，并没有带来很好的效果，于是才有今年 3 月垃圾邮件引发的事件。

团结就是力量

中国互联网协会副秘书长黄澄清指出：“全面彻底反垃圾邮件，要标本兼治，除了技术上加大投入以外，更重要的是全行业协调配合，同时，加强公众教育也是同等重要的。”此次互联网协会的反垃圾邮件协调小组起草了“反垃圾邮件规范”，以保护我国电子邮件用户的正当权益，促进电子邮件服务业的正常发展。规范要求邮件服务提供者建立垃圾邮件的信息收集、反馈和处理机制等，协会将与其他国家和地区

的反垃圾邮件组织进行沟通和联系，协调协会成员和其他国家和地区的反垃圾邮件组织和服务提供者之间的关系。此次互联网协会的行动我们可以看作是反垃圾邮件的一次总动员，希望我们不必走到法律护航的那一步，从行业的自觉性行为转化为公众的共同行为，大家都来反对发送、转发垃圾邮件，为净化网络环境做出我们的贡献。

关机也能被窃听手机泄密成信息安全隐患

你能想得到吗？小小手机随时随地都有可能带来泄密的危险，而且已有越来越多国家对手机失泄密问题予以关注并警惕。

北京晚报 11 月 11 日刊登有关报道，国防大学李大光副教授专门分析了手机失泄密的原因。李教授在文章中说，手机通信是一个开放的电子通信系统，只要有相应的接收设备，就能够截获任何时间、任何地点、任何人的通话信息。

有人认为，那我不通话，你不就什么也窃听不到了吗？李教授说，其实不然，因为在待机状态，手机也要与通信网络保持不间断的信号交换，在这些过程中产生的电磁频谱，人们很容易利用侦察监视技术发现、识别、监视和跟踪目标，并且能对目标进行定位，从中获得有价值的情报。

李教授还介绍，即使关闭手机，利用现代高科技，持有特殊仪器的人，仍可遥控打开手机的话筒，继续窃听话筒有效范围内的任何谈话。也就是说，使用者只要将手机放在身边，就毫无保密可言。

专家指出，惟一保密的办法就是在特殊的场合将手机电池取出，彻底断绝手机的电源。一些国家的情报部门、军方和重要政府部门，都禁止在办公场所使用移动电话，即使是关闭的手机也不允许带入。

ISS：新缺陷会触发更多的网络攻击

互联网安全系统（ISS）公司于当地时间 11 月 12 日透露了互联网域名系统所依赖的软件中包含的3个安全缺陷。

ISS 公司称，这三个缺陷可能会使大多数的互联网域名系统（DNS）服务器受到

拒绝服务攻击（DoS）。一个安全缺陷允许黑客在存在该缺陷的计算机上运行任何代码。ISS 警告说，考虑到 3 周前针对 DNS 根服务器的攻击，可能很快会有新的攻击发生。

ISS 安全缺陷研究业务部门的负责人丹表示，使用这一缺陷能够开发出蠕虫病毒，我们认为这一安全缺陷与导致红色代码病毒的安全缺陷在同一个水平上。

这些缺陷出在普及的“伯克利互联网域名”（BIND）软件。运行版本号在 4.9.10REL 和 8.3.3REL 之间的该软件的服务器需要安装相应的安全补丁程序。尽管该软件的最新版本是 BIND9，许多系统管理员仍然使用 BIND8，许多更“陈旧”的系统还在运行 BIND4。

ISS 的丹表示，目前有数万至数十万台与互联网相连的服务器运行 BIND 软件。

尽管发生在 10 月份的对互联网 DNS 根服务器没有利用任何安全缺陷，但美国联邦调查局（FBI）和系统审计网络安全研究所多次警告，没有安装补丁程序的 BIND 软件中的安全缺陷位居互联网上 Unix 系统的 10 大安全缺陷之列。

负责管理开放源代码 BIND 软件的互联网软件协会建议，系统管理员应当将软件升级到 BIND9.2.1。

英国黑客多次入侵美军网络最多将被判 70 年

美国检察官周二起诉一名英国男子入侵近百台政府和私有企业的计算机，干扰了军方的工作，在过去一年中造成了 90 万美元的损失。

加里麦金农是一名生活在伦敦的失业程序员，弗吉尼亚州的检察官表示他不仅在珍珠港、康涅狄格等几处军事基地盗取密码、删除文件、监视访问、关闭

计算机网络，还入侵了 NASA、田纳西大学、宾夕法尼亚州的一家图书馆和几家私有企业。

麦金农在新泽西州也受到了七项计算机诈骗罪的指控，如果罪名成立，他最多可能被判入狱 70 年，罚款 175 万美元。

根据指控，麦金农从 2001 年 3 月到 2002 年 3 月一共入侵了 92 个计算机系统。入侵后，他用名为“RemoteLyAnywhere”的软件监视网络访问并删除文件。他下载了数百个用户密码，还破坏了几个关键文件使计算机无法工作。有一次，他使华盛顿地区 2000 名军方用户三天无法上网。还有一次，他使美国海军在新泽西的军事基地蒙受了 29 万美元的损失。

美国司法部一名女发言人表示，麦金农没有侵入任何机密信息，但是安全专家指出：“如果能影响军方的关键系统，我就认为这是严重的黑客攻击。”

赛门铁克推出集中开放式信息安全管理系统

近日，互联网安全技术与解决方案供应商赛门铁克公司宣布推出业界第一个集中开放式的信息安全管理系统——赛门铁克安全管理系统。该系统包括一整套管理应用软件，能够对企业信息安全设施进行积极控制，为企业信息主管更好决策提供信息，从而提高企业信息安全环境的有效性。

赛门铁克公司执行副总裁 GaILHamILton 说："我们的客户所面临的首要挑战就是如何管理其复杂的安全基础设施及其已经部署的众多安全设备所产生的巨大数据流，赛门铁克的方法是为用户提供开放式政策和事故管理能力，使他们能够积极地保护其网络不受已知威胁的攻击，并对未知的新型攻击保持实时响应。"

今天管理企业安全是一个艰难的过程，需要将缺乏集成和互操作性的不同厂商的不同产品进行综合。其结果是复杂性加剧和运营成本增加，而且在做出重大安全决策时不得不依赖孤立的安全数据。对于大多数企业而言，这就意味着弱势安全风险侧面——业务基础设施不安全，遵循规章不到位，安全审查失败和安全管理成本激增——这是不符合业务要求的。而使这一过程更为艰难的是要在整个企业浏览系统和网络信息流中保护产品，并就每一个可疑行动发出信息。每一个信息都被称做一个安全事件，即便是中等规模的公司每个月也会出现一千万起这样的事件，它可能是表明缓冲区溢位攻击的畸形或超长网络包，也可能是影响重大或无关紧要的登录失败。总之，很难决定一个既定事件会不会带来麻烦。而事故是指需要应对并加以解决的事件或形势。主动攻击或病毒爆发

通常都是由一个或多个事件组成的事故。已知的系统漏洞或已被发现的违反政策行为都应被视为需要快速响应的事故。然而，问题的关键就难在要在数以百万的事件中及时发现事故并采取行动。

赛门铁克安全管理系统可以帮助企业解决这一难题，它诉求一种全面的安全形势观，通过全面安全管理的方法告诉企业的信息主管们——“我的企业到底有多安全？”、“我应该把资源集中用于那里？”及“我是不是在尽我所能保护我的企业？”。这一业界首创的集成开放式的信息安全管理系统包括赛门铁克事件管理软件（SymantecEventManageRs）、赛门铁克事故管理软件（SymantecIncIdentManageR）和用于政策遵循的赛门铁克企业安全管理软件（SymantecESM）三个主要组成部分。用户可根据其业务目的选择并部署恰当的安全管理应用软件。

赛门铁克事件管理软件

如果您的企业只想全面了解某一具体保护领域内安全事件的情况，赛门铁克为这类企业用户提供了赛门铁克防病毒事件管理软件和赛门铁克防火墙事件管理软件。这些事件管理软件从赛门铁克和其他厂商的保护解决方案中整合数据，从而使用户能够全面掌握病毒和防火墙事件。用户还可搜集第三方厂商的

安全产品数据，包括 NetworkAssocIates 的杀毒数据和 CheckPoInt 的防火墙。额外数据搜集器有望在第四季度推出。赛门铁克正在与第三方厂商通过合作方案共同创造搜集器，该合作方案该方案的早期参与者目前包括开发主动网络防御系统的 TIpPingPoInt 和开发入侵预防软件的 EnteRcept，搜集器将于 2003 年第一季度正式宣布。

赛门铁克事故管理软件

对于拥有大型网络并每天碰到大量安全事件的企业用户来说，它们更加需要实时地全面掌握存在于网络层之间的安全数据及安全技术。赛门铁克事故管理软件提供开放式的实时事故管理，从而使企业能够最大限度地提升其安全技术的价值，发现并快速响应安全事故。

赛门铁克事故管理软件从不同厂商的众多产品和安全技术中发掘，整合安全事件并将之联系起来。它通过分析事件并找出它们的相互关系来确认事故，之后会一直跟踪每一事故的解决情况。它也允许根据事故的严重程度来决定事故的优先顺序，且在每一事故的生命周期中不断调整优先顺序。一旦发现事故，赛门铁克事故管理软件就会根据事故的具体特征提出专家指导意见，该指导意见的基础是公认最好的

SANS/CERT 事故响应框架。指导意见和针对客户的政策控制共同帮助安全人员快速有效地解决事故。系统所提供的指导意见也能帮助安全人员向一般的 IT 人员作出清晰全面的指示，这些指示能够指导他们具体地解决每一事故。

英国一网页设计师被控向全球传播电脑病毒

英国警方 13 日宣布，国内一名网页设计师因在全球范围内传播计算机病毒而被司法机关起诉。

被告西蒙瓦勒尔现年 21 岁，来自威尔士的兰迪德诺。今年 2 月，英国警方根据美国联邦调查局提供的情报将他逮捕。瓦勒尔被控非法袭击网站和在全球范围内传播两种以电子邮件为载体的计算机病毒，其中一种名叫“GOKARREDESI”的病毒影响了 46 个国家的计算机系统，是世界传播范围第三广泛的计算机病毒。瓦勒尔还被控私藏儿童色情照片。

瓦勒尔本月 8 日在伦敦获保释。他将于 12 月 20 日出庭受审。

十月互联网十大安全漏洞

十月份互联网上可考的信息安全漏洞共有 60 余条，本月 CNNS 安全专家经过认真研究和比较，评选出十条影响较大，严重程度较高的安全漏洞，并简单

地列出其原因和影响。从这些典型安全漏洞来看，互联网攻击手段越来越广泛，涉及到客户端安全，底层应用协议安全等等。此外，还有一个趋势是数据安全正成为信息安全的一个新焦点，它不仅包括数据库的安全，更包括数据的完整性，可用性，以及数据的监控和备份安全等。

所有具体漏洞的信息用户可参考 CNNS 漏洞信息库相关资料。

1.http://www.cnns.net/aRtIcLe/db/2659.htm

名称：phpBB2.0.0 用户权限可被非法提升缺陷

影响：phpBB 是一个在国外相当流行的电子公告板，而且该漏洞的攻击代码也随着漏洞的发布而同时公布出来了，采用受影响版本的服务器都可能受到攻击。

2. http://www.cnns.net/aRtIcLe/db/2657.htm

名称：多数厂商防火墙 FLood 攻击可导致状态表被填满

影响：防火墙广泛应用于边界网络保护，防火墙受到拒绝服务攻击将会导致受防火墙保护的所有网络不能正常访问网络资源。该漏洞既影响到网络关键设备，又影响了很多防火墙安全产品，影响极为严重。

3. http://www.cnns.net/aRtIcLe/db/2646.htm

名称：IE 浏览器被发现存在 9 处严重的安全漏洞

影响：IE 是微软 Windows 操作系统缺省安装的浏览器，该浏览器存在的多个安全漏洞将会导致浏览器客户端执行攻击者代码或泄露敏感信息。

4. http://www.cnns.net/aRtIcLe/db/2643.htm

名称：MicrosoftSQLServerWebtasks 权限非法提升缺陷

影响：多数 WINDOWS 系统平台数据库采用微软开发的 MSSQL 数据库服务器，该漏洞可能导致攻击者取得系统级的管理员权限，并且影响到 MSSQL7.0/2000 两个版本。

5. http://www.cnns.net/aRtIcLe/db/2615.htm

名称：SunSoLaRIs/bIn/Login 无需任何身份验证即可远程非法登录

影响：该漏洞其实是一个以前公布过的漏洞，但十月份公布的新的攻击手法将可能导致 SoLaRIs 服务器受攻击的影响面和可能性大大增加。利用该种新的攻击手法，任何入侵者将可能轻易取得 SoLaRIs 服务器用户权限。

6. http://www.cnns.net/aRtIcLe/db/2613.htm

名称：SQLServer 的多个安全缺陷允许获得缺陷服务器的控制权限

影响:MSSQL 服务器存在新发现的四个严重漏洞,微软为此开发出了针对所有以前 SQLServer7.0,SQLServer2000,MicrosoftDataEngIne(MSDE)1.0 以及 Microsoft Desktop EngIne(MSDE)2000 的补丁集。

7.http://www.cnns.net/aRtIcLe/db/2624.htm

名称:OutLookExpressS/MIME 数字签名缓存溢出缺陷允许运行任意指令

影响:OutLookExpress 客户端一直是病毒和黑客的流行攻击途径,该漏洞是一个相当典型而又极为严重的客户端攻击例子,利用 OutLookExpressS/MIME 数字签名缓存溢出缺陷,攻击者将能全权接控受害者机器。

8. http://www.cnns.net/aRtIcLe/db/2653.htm

名称:MITkRb5kadmInd4 溢出缺陷可获得 KDC 主机 Root 权限

影响:MIT 的 KeRbeRos 是一套非常著名的加密工具,一般用到此类加密工具的信息其敏感度都非常之高,成功利用该漏洞将能危及整个网络和数据的安全性、保密性。

9. http://www.cnns.net/aRtIcLe/db/2645.htm

名称:多家厂商 IPSec 的实现存在远程拒绝服务

攻击缺陷

影响：IPSec 是一套提供验证和加密功能，以确保信息秘密、完整地穿越公共 IP 网的 IP 安全扩展标准。该漏洞涉及到数据加密和用户身份验证，众多安全厂商在 IPSEC 的实现上都存在此漏洞。

10．http://www.cnns.net/aRtIcLe/db/2626.htm

名称：ORacLe8I/9ILIsteneRSERVICE_CURLOAD 远程拒绝服务缺陷

影响：ORacLe 数据库在大型数据存储检索中应用广泛，该拒绝服务漏洞涉及到 ORacLe 众多版本，对用户的数据的完整性、可用性将带来较严重影响。

ICANN 拟批准三个新的顶级域名

互联网域名管理机构 ICANN 已经建议采取有关步骤为网络导航系统增加三个顶级域名。ICANN 理事长 StuaRtLynn 上个星期发表了一份建议，即使在该组织准备评估去年增加同样多的域名所产生的效果时候，也提议准备增加新的网络域名。这份报告没有提到将要考虑的具体域名。

Lynn 在报告中写道，如果 ICANN 理事会希望这样做的话，这个建议为 ICANN 理事会提供了再征集三个域名的选择，经过合适的和短暂的竞标之后，再附加

某些条件。应当邀请前一轮域名申请人更新他们的建议并重新提出来，但是也欢迎提出新的建议。

顶级域名提供了网络地址系统最大的构件，规定了架构的一般种类，如.com、.edu 和表示机构的域名.gov 等。2000 年 9 月，ICANN 在原有的五个域名的基础上又批准了七个域名。域名还可以注册代表国家的顶级域名，如.uk 和.us。此外，美国的律师还建议为适用于家庭访问的网站增加.kIds 的域名。

2000 年年底，网络泡沫破灭之后，扩展网络域名被认为是保证地址系统健康的重要步骤。然而，随着数以千计的名称重新使用现有的域名，对新域名的要求也减弱了。

Lynn 在上星期的建议中表示，ICANN 的改革要使该组织把主要任务放在管理互联网域名方面，包括批准新的顶级域名。Lynn 表示，他建议加快准备的时间立即批准这三个顶级域名。

美众院批准耗资近十亿美元的网络安全法案

美国国会 12 日下午批准了一项大规模开支计划，该计划将支出近 10 亿美元用于电脑安全研究。

通过呼声表决，美众院通过了网络安全研究和发展法案（CSRDA），该法案在未来 5 年内将拨给大学约 9 亿美元用于创建安全中心、招募研究生以及支付研

究费用。

这些措施已得到参院的批准，将呈送总统布什签字。

在表决后举行的记者招待会上，该法案的支持者说，该法案有助于解决美国的“网络安全”问题，并相信会有更多的学生研究相关课题。

布什签署该法案后，该法案在 5 年内将达到以下目的：

拨款 2.75 亿美元用于博士后研究奖学金和高级研究奖学金。研究工作必须“与电脑系统安全有关。”

拨款 2.33 亿美元用于研究专用款项，研究内容包括 9 个与安全有关的领域，如密码、隐私、无线安全以及“提高发现、调查、起诉网络犯罪的执法能力，包括那些涉及知识产权保护的犯罪”等。

拨款1.44亿美元建立电脑和网络安全研究中心，该中心用于增加“电脑和网络安全研究人员以及其他专业人员的数量并提高他们的素质。”

拨款 95 万美元专项资金用于让大学“建立或改善电脑和网络安全的研究生和本科生计划”。

拨款 9000 万美元用于为那些追求电脑和网络安全研究的研究生建立培训计划。

拨款 3200 万美元研究资金，用于改善网络安全，

并支付“多学科、长期、高风险研究费用，以改善电脑系统的安全”。

拨款 2500 万美元用于培训计划，以鼓励研究生“在获得博士学位后选择网络安全为学术生涯”。

考生答卷被删 “黑客”破坏网上考试 被判刑 6 个月

近万考生答卷被删

今年 5 月 18 日上午，江苏省普通高中信息技术等级考试正在全省范围紧张地进行。参加此次考试的考生达 30 万人，整个考试都在网上举行。如此大规模的网上考试，不仅在全国属于首创，而且在国际上也很罕见。为此，江苏省教育厅购买了两台专用服务器，各地考点共用一个 FTP 用户和密码进行考生答案上传，汇总后进行网上阅卷。在系统安全方面，也请专家把关，力争做到万无一失。

作为江苏省教育厅会考办成员的诸老师，管理着全省各个考点上传的学生答卷信息。第一天考试前，诸老师一大早就来到机房检查电脑网络系统，确定全部运作正常。到中午，各考点的答卷大部分上传到了省考办的服务器上。然而，12 点 48 分，诸老师吃完午饭再次来到机房，对服务器上的数据进行查看时，突然发现部分上传数据发生丢失现象，遂立即分析服

务器的系统日志，结果找到了执行删除命令的日志行及进行攻击的 IP 地址。

正当诸老师与其他网管对这一现象进行分析时，当天下午 4 时 53 分，服务器上再次发生考生数据被删除的现象，作案方来自同一 IP 地址。这两次攻击，共删除了考试文件 100 多个，造成 85 所学校 9991 名考生的成绩被删除。

循踪发现作案嫌犯

公安人员接警后，迅速投入侦查工作。根据江苏省会考办提供的作案 IP 地址，警方与电信部门联系协查，确定当日使用该 IP 地址的是苏州某中学。随后，经过数天深入调查，公安人员发现该中学计算机教师罗某有重大嫌疑。经审问，罗某招供了所有犯罪事实。

原来，今年 4 月，罗某接到高二年级将进行全省信息技术等级考试的通知。由于机房的学生机都安装有硬盘保护卡，因此安装考试机软件的工作量较大。4 月 27 日，学校组织学生进行了第一次模拟考试，考完后向江苏省考试站点传送答卷，结果失败了。这时，罗某设法获取到上传时的登录账号和密码，然后再次进行了人工传输答卷文件，但仍未成功。这时，学校接到通知，要求重新安装考试软件以更新试题库，这

意味着所有工作得重头再来一遍。罗某对此十分厌烦，并冒出了恶作剧的念头。

第二次模拟考试后，罗某在苏州市教育局的指点下传送答卷成功。然而，在恶作剧念头的驱使下，罗某又设法获得了新的登录账号和密码，并当场删除了站点中的部分文件。此后，他接二连三地登录会考办的站点，下载文件、浏览目录、删除文件，在违法的泥潭中越陷越深。

5 月 18 日，正式考试开始了。担任监考的罗某在上午考试结束后，利用独自一人在办公室的时机，又登录到省考办的站点，进行了五六分钟的删除操作。下午考试结束后，罗某回到办公室，心中又冒出一个念头：把所有文件都删除掉。于是，再一次操作后，罗某删除了所有考生的文件。

补救及时数据恢复

第二天下午，苏州市教育局的有关教师到罗某所在学校检查系统日志，罗某意识到是在调查删除考试文件的事，紧张与害怕之下，试图逃避责任。次日，他即把安装在计算机中所使用过的与这次考试有关的软件、文件全部作了卸载，检查了可能留下的文件和注册表项，并复制了大量文件到硬盘中，尽可能清除痕迹，想以此逃避制裁。

然而，天网恢恢，疏而不漏。5 月 28 日，罗某被苏州市公安局沧浪分局刑事拘留。

据悉，考试文件被删除后，如果补救不及时，可能造成全省近万名考生重新参加考试，直接经济损失将达 20 多万元。幸而，经江苏省普通高中会考办公室组织各考点将备份文件重新上传，方将数据恢复。经过方方面面的努力，这起“黑客”操纵网络案的损失减少到了最低程度，但是，仍造成间接经济损失近 6 万元。

美国新法案规定黑客从严惩处可能终身监禁

按美国众议员在“家园安全部”法案中添加的新规定，计算机黑客将从严惩处，可能在牢里蹲一辈子。

众议院 13 日晚间以 299 票对 121 票，通过“家园安全部”DepaRtment of HomeLand Security）法案。该法案的目的在于，把一部分联邦政府组织整合成一个新的部，内含现有的 22 个联邦机构，包括情报局、海岸防卫队以及联邦调查局（FBI）的国家基础设施保护中心。

在展开辩论前的闭门政党协商中，众院共和党领袖在家园安全法案中插入了 16 页长的「网络安全加强法案“（CybeR Security Enhancement Act，简称 CSEA）。CSEA 旨在扩大警方不需先声请法院命令可径

行监看因特网或监听电话的职权，并赋予因特网服务供货商（ISP）更大的自由，把资料提供给警方。

今年 7 月间，全体众议院以 385 票对 3 票之差通过 CSEA，但此法案后来在参议院阵亡。让家园安全法案夹带 CSEA，支持者希望赶在国会休会前，让此法案二度闯关。

倡议 CSEA 的众议员 LamaRSmIth 说：”预防恐布分子可能随时以任何方法发动袭击，我们处理问题的方法需要改变。我们需要一个焦点清晰、任务明确的新政府组织架构，来保卫美国人民并加强公共安全。成立新的家园安全部，可履行那个重责大任。“

数月前，SmIth 曾表示：”在我们确保因特网基础设施的安全无虞之前，只消打几个键和连上网络，就足以瘫痪经济并危及生命。鼠标可能像子弹或炸弹一样危险。“SmIth 是众议院打击犯罪小组委员会主席，该小组委员会曾举办听证会，博得司法部高阶官员和微软、WorldCom 等主管支持 CSEA。

但基于隐私权顾虑，捍卫公民权的团体向来反对 CSEA 的部分条款。

”有很多不同的事情令人关切，但维护第四修正案和监听的标准规定，仍然是考验国会是否信守维护公民自由承诺的试金石。“电子隐私数据中心董事

MaRcRotenbeRg13 日说。

RotenbeRg 指出，CSEA 让 ”ISP 进一步向执法机关靠拢，牺牲了消费者的隐私利益。这或许不令人意外，但绝不是好消息 “。

民主党众议员 13 日抱怨，家园安全部法案的内容还来不及详读，就仓促付诸辩论。共和党代表则驳斥太草率通过此法案的论调。

CSEA 的内容

若获得参议员通过和总统签署成正式法律，此法将会：

让 ”鲁莽地 “置他人性命于险境的计算机闯入者终身监禁。法案附上的委员会报告指出，恐怖分子或网络攻击罪犯可能进一步伤害我国经济和重要基础设施，所以有必要从严惩罚，以加以防范。

允许警方在未取得法院命令的情况下有限度的监视，适用情况包括发现针对连网计算机 ”进行中的攻击 “活动，或 ”对国家安全利益立即的威胁 “。但监视范围局限于嫌犯的电话号码、因特网地址（IP）、网址（URL）或电子邮件主旨列信息，而非在线通讯或电话交谈内容。

修改现行怯律，让原本 ISP ”故意泄露 “使用者数据的行为合法化，适用范围除了原本即获准的情况

（像是解决技术瑕疵、接获法院命令或协助警方查办现行犯）外，另增加「涉及他人生命危险或严重肢体伤害、需要立即揭露数据」的紧急事件。

明定现行禁止电子监听设备广告的命令的适用范围扩及在线广告。此禁令目前只涵盖报纸、杂志、传单及其它出版品。

网络安全 8 大趋势

2002 年，防火墙、入侵检测、防病毒、加密四大产品成为市场的主流。专家预计，到 2003 年，安全市场将增至八大件。

一、物理隔离

解决方案：物理隔离网闸

物理隔离与逻辑隔离有很大的不同。物理隔离的哲学是不安全就不连网，要绝对保证安全。逻辑隔离的哲学:在保证网络正常使用的情况下，尽可能安全。两者是完全不同的产品。

物理隔离的思路，源于两台完全不相连的计算机，使用者通过软盘从一台计算机向另一台计算机拷贝数据，有时候大家形象地称为“数据摆渡”。由于两台计算机没有直接连接，就不会有基于网络的攻击威胁。

二、逻辑隔离

解决方案：防火墙

在技术上，实现逻辑隔离的方式有很多，但主要是防火墙。防火墙在体系结构上有不同的类型:有双网口、有多网口、DMZ 和 SSN。不同的类型在 OSI 的 7 层模型上工作机理有明显的不同。

防火墙的主要评价体系包括：性能、安全性和功能。实际上，这三者是相互矛盾、相互制约的。功能多、安全性好的技术，往往性能受影响；功能多也影响到系统的安全性。

三、防御来自网络的攻击

解决方案：抗攻击网关

网络攻击特别是拒绝服务攻击（DoS），利用 TCP/IP 协议的缺陷，有些 DoS 攻击是消耗带宽，有些是消耗网络设备的 CPU 和内存。其中，具有代表性的攻击手段包括 SYNfLood、ICMPfLood、UDPfLood 等，其原理是使用大量伪造的连接请求报文攻击网络服务所在的端口，比如 80，造成服务器的资源耗尽，系统停止响应甚至崩溃。而连接耗尽攻击，则使用真实的 IP 地址，发起针对网络服务的大量的真实连接来抢占带宽，也可以造成 Web 服务器的资源耗尽，导致服务中止。其他一些利用网络协议缺陷进行攻击的 DoS 技术包括 Land、WinNuke、PingofDeath、TeaRDRop

等。

抗攻击网关能识别正常服务的包，区分攻击包。目前 DDoS 的攻击能力可达到 10 万以上的并发攻击，因此抗攻击网关的防御能力必须达到 10 万以上。

四、防止来自网络上的病毒

解决方案：防病毒网关

传统的病毒检测和杀病毒是在客户端完成。但是这种方式存在致命的缺点，如果某台计算机发现病毒，说明病毒已经在单位内部几乎所有的计算机感染了。如果病毒是新的，旧的杀病毒软件一般不能检测和清除。

应在单位内部的计算机网络和互联网的连接处放置防病毒网关。如果出现新病毒，只需要更新防病毒网关，而不用更新每一个终端软件。

五、身份认证

解决方案：网络的鉴别、授权和管理（AAA）系统

80%的攻击发生在内部，而不是外部。内部网的管理和访问控制，相对外部的隔离来讲要复杂得多。外部网的隔离，基本上是禁止和放行，是一种粗颗粒的访问控制。内部的网络管理，要针对用户来设置，你是谁？怎么确认你是谁？你属于什么组？该组的

访问权限是什么？这是一种细颗粒的访问控制。

在一般人的心目中，基于 Radius 的鉴别、授权和管理（AAA）系统是一个非常庞大的安全体系，主要用于大的网络运营商，企业内部不需要这么复杂的东西。这种看法越来越过时，实际上单位内部网同样需要一套强大的 AAA 系统。根据 IDC 的报告，单位内部的 AAA 系统是目前安全市场增长最快的部分。

六、加密通信和虚拟专用网

解决方案：VPN

单位的员工外出、移动办公、单位和合作伙伴之间、分支机构之间通过公用的互联网通信是必需的。因此加密通信和虚拟专用网（VPN）有很大的市场需求。IPSec 已经成为市场的主流和标准，不是 IPSec 的 VPN 在国际上已经基本退出了市场。

VPN 的另外一个方向是向轻量级方向发展。

七、入侵检测和主动防卫（IDS）

解决方案：IDS

互联网的发展，已经暴露出不可避免的缺点:易被攻击，技术人员的好奇和技术恐怖主义使金融机构、企业、学校等单位很难避免。

针对黑客的攻击，从技术路线上来讲，早期的思路是加强内部的网络安全、系统安全和应用安全，安

全扫描工具就是这样一类产品。但是，扫描是一种被动检测的方式，入侵检测和主动防卫（IDS）则不同，是一种实时交互的监测和主动防卫手段。

八、网管、审计和取证

解决方案：集中网管

网络安全越完善，体系架构就越复杂。管理网络的多台安全设备，需要集中网管。集中网管是目前安全市场的一大趋势。

从来就没有一种技术可以绝对保证网络安全。如果执行人员出现失误，实际的网络安全也就存在问题。因此，技术越先进，审计功能就变得越重要。

审计并不完全是检查安全问题。对审计的数据进行系统的挖掘，还具有非常特殊的意义，比如，可了解内部人员使用网络的情况，或对外部用户感兴趣的公司产品和内容进行总结，了解用户的兴趣和需求等。

微软对其安全努力充满信心

据微软公司官员称，在微软公司董事会主席比尔盖茨要求公司雇员制作更加可以信赖的Windows十个月之后，这个可信赖计算计划正在得到回报。

微软公司负责高级战略和政策的高级副总裁CRaIgMundIe在每月举行一次的微软公司硅谷系列演

讲中表示，微软公司的可信赖计算计划已经取得了进展。其它公司必将效仿微软公司的做法，否则就可能失去消费者的信任。

微软公司努力的亮点之一是制作了错误报告软件。这个软件允许志愿者使用 WindowsXP 操作系统让他们的计算机自动报告可能造成应用程序崩溃的任何软件瑕疵。

由于微软公司新的计划把找软件瑕疵当成了一项优先的任务，这个软件还能在消费者完全失望之前，解决一些安全问题。

这个收集瑕疵的软件已经证明，将近 50%的系统崩溃问题是由 1%的应用程序错误引起的。排在前 20 位的错误占所有问题的 80%以上。

Mundle 表示，微软公司的安全努力不是没有代价的。在盖茨提出可信赖计算计划不久，微软公司便停止了 Windows 的开发，以便对开发人员和项目人员进行安全编程培训。这个计划的总费用超过了 1 亿美元。

微软公司还推迟了下一代的.Net 服务器软件。推迟的原因就是微软公司新的重点是注重安全。

微软公司还逐步淘汰了老版本的、安全漏洞较多的 Windows 操作系统。尽管这种做法不太受欢迎。微软公司不再支持 Windows95 操作系统，对最近影响该

系统的安全漏洞不再提供补丁，尽管这种操作系统还有人使用。

Mundle 表示，这种做法是可信赖计算计划的一部分，是要保证目前使用的系统更加安全。

FTC 对垃圾邮件和网络诈骗实施第三次打击

以美国联邦贸易委员会为首的政府有关管理部门 11 月 13 日宣布对网络垃圾邮件制造者和网络诈骗分子实施打击行动。

美国的这些管理机构宣布，他们一共采取了 30 多次执法行动，向大约 100 多个垃圾邮件制造者发出警告，警告他们停止发送人们不需要的并且常常带有欺骗性的商业电子邮件信息。另外，这些管理机构宣布，对垃圾电子邮件的调查结果表明，那些在聊天室和新闻组等公开场合公布自己邮件地址的网络用户收到垃圾电子邮件的可能性最大。

联邦贸易委员会的律师 BRIanHuseman 表示，这是美国联邦贸易委员会今年组织管理部门实施的第三次打击垃圾电子邮件的行动。他说，对于这个问题，联邦贸易委员会将加强执法和对消费者的教育。

虽然加利福尼亚等州实施了禁止垃圾电子邮件的法律，但是，美国联邦法律还没有相应的条款。尽管如此，联邦贸易委员会还是有权与欺骗性行为、欺

骗性广告和直接的诈骗作斗争的。

联邦贸易委员会采取的法律措施通常是民事诉讼形式而不是刑事诉讼。投诉要使有罪的方面作出赔偿和停止其活动。

联邦贸易委员会在 11 月 13 日的声明中还说，它对一位名叫 BRIanSILveRman 的曼哈顿人提出了起诉。这个人从今年 1 月起在 eBay 网站拍卖笔记本电脑，欺骗了 200 多人，骗取现金大约 30 万美元。SILveRman 要求竞买者用支票和汇款单支付。他却不给电脑。法律人士指出，消费者应该找用信用卡支付的卖主，这是保护自己的最好的方法。

为了研究垃圾电子邮件，联邦贸易委员会和州管理部门在互联网上贴出了 250 个电子邮件地址。其中，在聊天室里贴出的电子邮件地址 100%收到了垃圾电子邮件。在新闻讨论组中贴出的电子邮件地址有 86%收到了垃圾电子邮件。在免费个人网页上贴出的电子邮件地址有 50%收到了垃圾电子邮件。

联邦贸易委员会的律师 Huseman 介绍说，垃圾邮件的发送者是使用自动的软件程序，在网上搜索“@”符号得到这些电子邮件地址的。如果消费者在网上公开他们的电子邮件地址，这种程序就能收集到。

参加这次打击垃圾邮件和网络诈骗活动管理机

构除了美国联邦贸易委员会之外，还有美国邮政检查署等十几个单位。

SUN 首席科学家：安全计算需要共同参与

在 ORacLeworld 大会上发言时，Sun 公司的首席科学家、兼该公司研究院的主管约翰盖奇建议，应当由全社会共同参与，促进安全计算的发展。

在强调安全仍然是一个全球性的挑战时，盖奇引用了最近对互联网 DNS 根服务器发动的大规模攻击，他说，社会的参与有助于解决这样的问题。

盖奇提到了政府在提高安全性方面所作的努力。他表示，计算机专业人士需要向公众透露所掌握的安全缺陷的资料，才能提高安全性。

他还对甲骨文公司将一个可伸缩的Linux系统称为“攻不破的 Linux ”的作法持不同意见。他还表示，与 SoLaRIs 不同，微软公司的 Windows 操作系统是不安全的。SoLaRIs 在开发时就充分考虑了安全性。通过不断地美化Windows永远也不可得到用户所期望的安全性。

盖奇还对戴尔公司的主席兼 CEO 迈克尔戴尔将 Linux 认为是 UnIx 的说法进行了批评，他说，戴尔先生应当明白，Linux 和 UnIx 不是一回事儿。在周二的讲话中，戴尔将 Linux 称作是专有 UnIx 的超级替补，

并把它称为新的 Unix。

并非事不关己！全球 13 台路由器同时遭袭击

美国当地时间 10 月 21 日，全世界 13 台路由 DNS 服务器（RouteServer）同时受到了 DDoS（分布式拒绝服务）攻击。值得庆幸的是并没有酿成严重事故。但此事再次表明，在因特网上目前仍旧存在很多充当 DDoS 攻击帮凶的机器。每台机器的预防策略的不完善就有可能威胁到因特网赖以存在的基础。因此在本栏目中，笔者在介绍这次事件的同时，将向大家解释一下预防此类事件发生的措施。

被瞄准的路由服务器

对于本栏目的读者来说，勿需再解释 DNS 服务器的重要性。为了使用 Web 和邮件等各种服务，解决名称问题的 DNS 服务器是不可缺少的。其中，采用分级结构的 DNS 服务器主干部分的路由服务器如果无法正常运行，那么因特网就会陷入瘫痪。此次攻击的目标就是这种路由服务器。

路由服务器在全球只有 13 台。如果这些机器全部陷入瘫痪，那么整个因特网都将陷入瘫痪。在 13 台路由服务器中，名字分别为“A”至“M”，其中 10 台设置在美国，另外各有一台设置于英国、瑞典和日本。下表是这些机器的管理单位、设置地点及最新的

IP 地址。其中，IP 地址等参考了“named.Root”文件。

总之，实际上相关技术人员一致认为此次攻击根本不值得去小题大做。

不过，如果仅从此次事件的“后果”来分析，就认为“不会所有的路由服务器都受到攻击，因此可以放心”，或者“路由服务器产生故障也与自己没有关系”，还为时尚早。此次事故的发生原因不在于路由服务器本身，而在于因特网上存在很多脆弱的机器。

罪魁祸首是因特网上脆弱的机器

请允许笔者再重复一下，路由服务器此次受到的攻击是 DDoS 攻击。这就是说，通过向因特网上脆弱的机器中植入 DDoS 客户端程序（如特洛伊木马），然后同时向作为攻击对象的机器发送信息包，从而干扰对象机器的服务（据称此次的攻击使得路由服务器所接收到的信息量达到了平常的 30—40 倍）。

此次事件绝对不是因为路由DNS服务器太脆弱而导致的。其原因是因特网上被植入 DDoS 客户端程序的机器太多。因此这次事件对普通服务器管理员来说，也不无关系。

机器的脆弱性被利用来植入 DDoS 客户端程序已不是什么新鲜事。目前已经公开的、由供应商提供补

丁程序和修正版本的脆弱性就有很多。但正是因为没有针对这些脆弱性采取措施，才导致了路由服务器遭受攻击。

除服务器管理员外，对于普通用户来说，也并非事不关已。目前基于 ADSL 和 CATV 的永久网络接入已经非常普及，由此客户端机器也完全有可能变成实施攻击的帮凶。因此作为防止脆弱性的措施，最重要的是，不仅要防止自身的机器免受入侵，还要防止成为别人实施攻击的帮凶，说得严重一点，也是为了自身能够顺利地连续使用因特网。

尽管此次事件并不是所有路由服务器都受到了攻击，但今后如果这种情况——在因特网上到处都有脆弱的机器——继续下去的话，那么就极有可能因更“强大的”攻击方法的出现，而导致异常严重的事态。认识到这一点后，每台机器就必须采取防止脆弱性的措施。希望大家把预防脆弱性措施看成是将机器接入因特网时所必须承担的责任。

日美两国应对措施截然不同

最后，笔者想介绍一下在此次事件中，日美两国在应对方面表现出的不同态度。在美国，由于考虑到此次攻击可能是服务器恐怖袭击，因此美国白宫和 FBI 等正在对事件进行调查。当然，除了担心服务器

遭受恐怖袭击外，另一个原因是 13 台中的 10 台集中在美国。

而在日本，并没有见到任何有关政府采取行动的报告，而只是全权委托WIDEPRoject来负责调查此事。另外，日本国内的部分专家还警告说："现在大家对服务器恐怖袭击表现得过于神经过敏"。

不管此次攻击到底是不是服务器恐怖袭击，每个管理员和用户应该做的是，采取措施不让自己的机器成为别人实施攻击的帮凶。

W3C 联盟规范网络服务标准

网络业界主要标准组织周四发布了关于网络服务结构的一组文件，该组织做出了前所未有的努力来使网络服务体系标准化。

World Wide Web 联盟（W3C)提出了网络服务结构文件的第一个工作草案和网络服务结构规范的第四版。网络服务的定义是准许开发者构建软件，以便让具有不同计算系统的公司可通过网络互动并开展电子商务。

结构草案是一个关于网络服务构成与企业间如何互动的技术指南。这个文件试图规定请求服务的系统与服务提供商之间的各种关系，还规定如何提供企业信息和如何得到这些信息。

有关操作要求的草案规定了结构草案必须涵盖的主题。此外 W3C 联盟还公布了第一个网络服务术语表的工作草案。该术语表的目标是将有关网络服务日益增长的行业语言规范化。

术语表奠定了迄今使用的网络服务专业术语的指针，术语表将敦促成员对新出现的定义保持谨慎注意，并且对正在使用的有分歧术语进行重新界定。

术语表现已进行了一些术语上的分类：结构和总体、技术定义、作用、服务特性，关于简单目标接入协议（SOAP)的特别标准、安全与隐私术语和管理术语。

草案所界定的术语既有普通的，也有不熟悉的。对“choreogRaphy”的解释就有了发展，这是指“从某一相应节点发出的订货信息详述或多节点集成”。还有，“终端用户”被定义为“为应用目的而使用资源的自然人”。

原 ExcIte@Home 公司股东指控 AT&T 诈骗和偷窃技术

破产的 ExcIte@Home 网络公司的受害的投资者称，历时一个月的调查发现的新的证据表明，AT&T 公司从事了“诈骗”和企业“技术偷窃”行为。

股东们 11 月 14 日向纽约联邦法院对 AT&T 公司

和前公司董事提出了起诉。起诉中新的错误行为的细节多数是根据采访原Excite@Home公司雇员和前首席执行官 PattIHaRt 的结果整理的。

这个修改的起诉书指控 AT&T 公司高级管理人员制定了一个计划，窃取用于开发有竞争力的宽带网的关键的知识产权。早在 2002 年 2 月，AT&T 公司就制定了名为“汽艇计划”的有线互联网试验计划。第二个月，该公司就制定了一个计划复制和改用了 Excite@Home 公司的技术。

原告律师称，这个修改的起诉书包含了这个案子中的重要的新证据。

股东集团法律小组委员会主席 FRankThomas 说，我们认为，我们没有过硬的证据是不会到法院来的。我们都在谈论AT&T公司的角色并能说出有关的理由。但是，现在，我们有证据来证明这些说法。

AT&T 公司不愿意对这个即将审理的案子发表评论。

股东们的联合起诉只是Excite@Home公司灭亡之后悬而未决的事情之一。Excite@Home 公司演绎了网络时代最具传奇色彩伊卡罗斯的故事。即使在这家公司的用户转移到其它网络服务提供商一年以后，许多批评家还认为，这家公司的破产也许是可以避免的。

Excite@Home 公司曾是最大的宽带互联网服务提供商。一年前破产时，股东们和债券持有人都指责 AT&T 公司帮助策划了 Excite@Home 公司的破产，或者至少从该公司的破产中得到了好处。

股东们在起诉书中还例举了具体的例证。从 2001 年开始，AT&T 公司的人员就要求拷贝 Excite@Home 公司关键的软件和数据，包括配置数据库、工程和规划文件。这些要求虽然遭到了 Excite@Home 公司雇员的反对，但是最后还是得逞了。

股东们说，到 2001 年春夏之交的时候，也就是 Excite@Home 公司破产之前，AT&T 公司已经能够把 Excite@Home 公司的通信转到该公司的服务器上了。这就使用户转换到 AT&T 公司网络的工作变得非常简单了。

这些行为多数都是 AT&T 公司在 2001 年 2 月安插在 Excite@Home 公司担任负责宽带网服务的临时副总裁 HosseInEsLamboLchI 的指导下干的事情。

批评人士一直对 EsLamboLchI 的任务表示怀疑。他们指责他用从 Excite@Home 公司收集来的技术帮助 AT&T 公司建立自己的网络。

这个联合起诉小组大约由 200 名个人股东组成。他们声称，他们有证据表明 AT&T 公司、Excite@Home

公司的前管理人员和董事有证券诈骗行为。

法院对这起投诉的听证会日期还没有确定。纽约南区联邦法院将负责审理此案。

政务内外网应一头大 专家呼唤相关标准出台

国家有关部门颁布了政务内网应与政务外网物理隔离的规定。那么，政府机关在建网时应注意些什么呢？11 月 14 日，本报主办的“电子政务内、外网隔离应用现场交流会”在社科院网络中心举行，交流了政府机关建网的经验和体会。代表们认为内外网隔离的一个解决方法，就是政府机关在建网时，相互隔离的电子政务内、外网应该是“一头大”。也就是说，其中一套系统很大，成为主要部分；而另一套系统则相应很小。

“一头大”是与“两头大”（内、外网两套系统都具备相当规模）相对的。它之所以是一个比较好的解决之道，是因为两头大不光需要较大的投入；而且，这两个网之间的信息交换会成为一大难题。目前，如何界定内网和外网还缺少权威的判定，与会的用户代表对此提出了两种做法。一种办法是尽力缩小外网，集中力量建设内网；另一种办法则是把内网的内涵缩小，将其归结为需要传递机密信息的小范围网络；同时，将外网包括的范围扩大，使得政府机关大多数人

员的办公在此网上进行。这样，核心的涉密网很小，而处理日常事务的网很大，也可以以较少的投入解决问题。

会上代表们还达成了其他一些共识。例如有的代表指出：物理隔离还是有必要的，但物理隔离不能无限制扩大，不能凡是不同性质的网就隔离起来，必须注重网络的可用性。如果某些信息是属于核心机密的话，甚至可以干脆不使用计算机。如果考虑到要联网的话，就不能不注重网络的可用性。有的代表认为，物理隔离在现阶段是解决安全隐患的最好方式，但是目前内外网物理隔离只到 47 个省部级，再向下的部门与上级单位如何互联？目前内外网的功能定义和范围还不太清楚，由于没有相关标准，基本上是各单位自己界定，影响了各部委之间的资源共享，因此呼吁国家有关部门尽快出台相应标准和措施。农业部信息中心方瑜主任还提出，单位内部不要为了自己的利益，或所谓的“权威性”，把本来不属于机密的信息，自设成小团体的“涉密”网。

与会代表的意见也出现了一些分歧。如有的代表提出，一个单位的网络是否具有足够的安全性，也应该有权威部门作出判别和认证。但另一些代表指出：绝对的安全是不存在的，在安全问题上不能存在依赖

思想。如果大家都坐等国家拿出相应的解决办法出来，就什么事都干不成了。各单位应该结合自己的实际情况，探索出适合自身的解决办法。

来自农业部、铁道部、国土资源部、水利部、国家工商总局、广电总局、环保总局、国家计生委计财局的十几位专家和 IT 厂商参加了本次现场会。

日本为加强网络安全保护正考虑不采用 Windows

美国太平洋时间 11 月 16 日(北京时间 11 月 16 日)消息，日本政府将考虑用另外一种操作系统替代微软公司的 Windows 操作系统，以便加强计算机网络安全保护。

保护计算机网络安全是日本首相小泉纯一郎建立“电子政府”计划的一个长期目标，这一“电子政府”计划允许公民通过互联网与政府各部门进行工作交流。目前，日本政府计算机网络中使用的服务器和个人电脑中，绝大多数都在使用 Windows 操作系统。但是，日本政府对于采用其它的操作系统却很感兴趣，特别是一些开放源文件程序，如 Linux。开放源文件程序的优势就在于，它们与微软公司的软件产品不同，它们不需要用户支付许可证费用，并且可以修改，因为它们的源文件代码都是免费的。所以，系统

操作者就可以很容易地应付他们面临的各种问题。

从明年 4 月份开始的下一财年中，日本公共管理部门、内政部门、邮政及通讯部门都将建立专家小组，对其它国家如何使用开放源文件操作系统的情况进行研究。公共管理部门的官员们没有就此事立即发表评论。日本政府对于计算机网络安全的关注是从今年 8 月份开始的，当时日本军方使用的一个计算机网络数据发生了泄密事件。就在数据丢失事件的前一天，日本政府刚刚引起公民身份证识别系统，可以通过网络跟踪公民个人数据，通过 11 位数字识别每个日本公民的身份。但是，数据丢失事件发生后，许多地方当局拒绝使用这一系统，原因是害怕被黑客攻击。

Sun 联合 CheckPoInt 推出基于 Linux 的网络安全设备

周一，Sun 公司宣称，该公司同以色列防火墙厂商 CheckPoInt 软件公司联手开发了一种基于 Linux 的安网络全设备。

这款新产品名为 SunLX50FIRewall/VPN，它采用增强了安全功能的 Linux 源码开放系统，以及 CheckPoInt 公司的防火墙和虚拟个人网(VPN)软件，该设备可以保护企业网络通讯安全。

基于 Sun 公司的 LX50 英特尔芯片服务器的这一

新产品支持 CheckPoInt 安全开放平台规范(OPSEC)，这样就可以与其它软硬件厂商的产品集成。

去年 2 月份，当 Sun 宣布开始销售基于 Linux 的服务器时，在业界石破天惊。在 8 月份举办的 LinuxWorld 大会上，该公司展示了 LX50 服务器，该服务器同时支持 Linux 和 Sun 自己的操作系统 SoLaRIs9。

Sun 预计在 Comdex2002 大会中首席执行官 ScottMcNeaLy 的主题演讲时展示这一网络安全设备。

这一新设备预计在 2003 年一月份上市，起价为 3300 美元。

综述：阻击网络安全头号威胁

10 月 21 日下午 5 点前后，全球互联网的核心基础设施遭遇了一场最严重的攻击。分布全球的 13 台互联网根服务器均受到大规模 DDoS(分布式拒绝服务)攻击，数不清的 ICMP 报文，如洪水一样，冲击着重重保护下的根域名服务器。事后安全专家心有余悸的说，只要攻击再持续一个小时，整个互联网的域名服务体系就会陷入崩溃。其实，类似的攻击，在网络上已经屡见不鲜。

2000 年初，全球顶级的网络服务商，yahoo,ebay,amazon,Microsoft 先后遭到大规模

DDoS(分布式拒绝服务)攻击，加速了脆弱的网络经济的崩溃。美国参议院联合经济委员会主席、犹他州参议员 Rob.RtBenn.tI 事后说：最近那些针对大型商业网站的“拒绝服务”攻击，会削弱公众对互联网以及通过其所从事商业交易的信心。

2000 年中美黑客大战，中国一些黑客通过拒绝服务攻击的方式造成美国白宫及多家美国政府部门的站点瘫痪，引起了美国国家安全机构的极大重视。

2001 年 2002 年，著名网络服务商 www.8u8.com 遭受拒绝服务攻击打击，事后该公司悬赏几十万元追查肇事者，并向公安报案，但是最终未能抓获任何嫌疑人。

2002 年，高考结束后，两省高教局开办的网上查分系统遭受猛烈的拒绝服务攻击，当地教育网对外服务无法开展，几乎无法完成后来的网上招生工作。

2002 年 7 月，全球活跃程度排名第三的病毒，由印度激进分子制作并传播的 Yaha，在传播的同时对巴基斯坦政府站点进行拒绝服务攻击，传播范围更大，攻击力更强，更加大了拒绝服务攻击的防护难度和追查难度。

拒绝服务攻击(DenIaL of Service，简称 DoS)正在肆无忌惮地侵扰着国内外著名的网络服务商和

金融证券、电信、政府等企业机构。2001 年，加州大学研究机构发布的一份报告中指出：世界范围内每周至少发生四千次拒绝服务攻击。随着许多关键性服务越来越多的普及上网，这种攻击形式带来的灾难性破坏和经济损失也将越来越大。不时发生的重大事件无疑不在提醒着人们：DoS 仍然是网络的头号威胁。

如何阻挡 DoS 攻击？已成为网络安全的最大难题，而国内更是连专业抗拒绝服务攻击的产品都没有。不过，日前，中联绿盟公司推出的专业防治 DoS 攻击的产品“黑洞”CoLLapsaR 填补了这一市场空白，实现了在高强度攻击环境下，保持 95%以上的连接保持率和新连接发起成功率。

头号威胁带来的安全需求填补国内市场的空白。绿盟科技显然明白这对信息安全产品市场的重大意义和背后隐藏的巨大商机，并希望通过“黑洞”CoLLapsaR 产品的推出，来满足市场上因 DoS 攻击的巨大威胁而带来的广泛安全需求。

所谓 DoS 攻击，是指以阻塞服务器对正常请求的响应为目标的攻击途径，其中部分采用系统安全漏洞为切入点的攻击方式，可以很容易通过安装补丁，升级系统来防护；但是对于更多采用协议层的缺陷，或者采用资源比拼方式，以伪造过量请求造成服务器端

连接堆栈溢出或资源耗尽，达到攻击效果的攻击方法，多年以来一直没有很好的解决途径。

理解这种 DoS 攻击，可以想象为一个公用电话呼叫服务系统(比如 119 报警台)，如果有人控制了多部电话机，并利用它们恶意不间断连续拨打骚扰电话，就可能造成电话系统繁忙，从而阻塞正常的电话请求，造成呼叫中心无法为正常的用户请求服务。

就如同恶意骚扰公用电话系统只需拿起身边的电话一样，进行拒绝服务攻击的工具也极为泛滥，加上所针对的协议层的缺陷短时无法改变的事实，DoS 一直以来，都让网络安全领域束手无策，从 2001 年到现在，多家国内外安全站点都曾因拒绝服务攻击而饱受折磨，就是这一状况的真实写照。以最典型的 DoS 攻击 SYNFLood 为例，其原理及攻击源代码已经公布了好几年，但是直到今天依然具有极强的破坏力，国际上先后推出的诸如 RandomDRop、SYNCookIe，SynpRoxy 等等之类的防护算法也都无法根除这种攻击，在受到高强度 DoS 攻击的时候大部分防火墙对此也是无能为力，甚至成为攻击目标。

在“黑洞”这样的专业安全产品推出前，针对高强度 DoS 攻击现象，由于没有太好的解决途径，相当多遭受攻击的网络服务商只能无奈地采用增加系统

资源，扩充主机集群数量，采用负载均衡等方式的退让策略,希望通过提高主机集群的响应能力来被动缓解攻击。效果如何呢“这种做法在面临高强度 DoS 攻击的时候，其资源耗费和维护成本的增加往往是无止境的，而且攻击者往往得寸进尺，退让终究不是办法。”绿盟的工程师这样点评。

市场的需求是巨大的，网络安全厂商需要做的是如何阻击 DoS 攻击。就目前的市场而言，一些优秀的防火墙产品都内置了抗 DoS 模块，采用诸如 SynpRoxy、SyncookIe 或类似的算法进行有限类型的拒绝服务攻击的防护，并能够在中低强度的拒绝服务攻击环境下起到良好的防护效果。国外的专业抗拒绝服务产品也开始进入国内市场，并在一些大型网络服务商那里得到了实际应用。

但是，那些防火墙作为通用安全产品限于自身的功用性和处理事务的多样性，在抗拒绝服务这一具体环节上根本无法达到高强度防护的能力；而国外的同类产品其昂贵的价格和并不过人的防护能力显然也仅仅是服务商在经受攻击困扰而又没有选择余地情况下的无奈之选。“黑洞 ”CoLLapsaR 的出现打破了这种格局，它为所有网络服务商和将关键性服务上网的金融证券、政府部门、电信、教育等各行业用户，以

及饱受拒绝服务攻击困扰并希望提升网络服务安全品质的企业，提供了全新的、更有效的选择。

阻击 DoS 攻击："道高一尺"还是"魔高一丈"

"黑洞"产品推出前，一些用户也在采用各种方式防范拒绝服务攻击，常用手段包括优化系统参数：比如减少连接等待时间，增加连接队列缓冲，减少和取消服务端连接重试次数，设置连接代理等等，优化参数只能有限提升系统的抗打击能力，可以对突发的拒绝服务攻击进行有限的抵抗，对于持续性的拒绝服务攻击，优化参数的防护意义几乎为零。

选用安全设备：具有抗 DoS 的防火墙在很多场合被用户采用，但是通用安全产品其所处理的数据种类繁多，其过滤规则和业务模式也非常繁杂，加上抗拒绝服务的认证和处理模块，系统整体性能将会极大下降，尽管可以很好保护所防护的主机，但是当攻击数据达到一定量级时，防火墙也会崩溃并造成受保护主机无法与外界通讯，从而实现拒绝服务攻击的效果。

增加资源，采用主机集群，负载均衡，DNS 轮循等诸多手段增加响应主机的数量和响应能力，期望超过攻击者的攻击能力，从而不影响正常响应，但是正如前面提到的，这种退让策略是无止境的。

对于企业而言，这些阻击 DoS 的技术方案和防护方法都过于繁琐、复杂。“对于大部分网络服务商、从事网络服务企业、信息交互企业以及政府机关等用户而言，他们所迫切需要的，不单纯是技术方案，更需要一种简化手段，能够在非技术人员值守，甚至无人值守的情况下，对多种拒绝服务攻击形式实现全自动的防护。”在经过市场调研后，绿盟作出了这样的结论。

基于这一市场迫切需求，绿盟推出了“黑洞”CoLLapsaR。据绿盟介绍，作为一个专业产品，黑洞的操作却非常简单，只需将外网和受保护网络通过黑洞的内外网卡互联，就可以完全实现对各种 DoS 攻击的智能分辨和自动防范。同时，管理者也可以通过管理端对黑洞进行灵活方便的配置，并能随时查阅当前流量状况、详细的日志和审计数据，从而方便追查肇事者，以法律手段打击网络犯罪。

另外，黑洞还可以通过不同的网络拓扑设置，能够保护的范围包括关键主机、网络设备(路由器、防火墙等)以至整个子网。黑洞的防护原理基于拥有国家专利的防护算法和先进的嵌入式体系结构，使用多种算法识别攻击流量和正常流量，能保证在很高的攻击流量环境下 95%以上的连接保持率和 95%以上的新

连接发起成功率，防护效率远远超过各种公开的防护算法和其他具有 DoS 防护功能的通用安全产品，与国际同类的专业抗拒绝服务产品相比具有明显优势。

目前，黑洞产品能够对包括 SYNFLood、ACKFLood、UDPFLood、ICMPFLood 和(M)StReamFLood 等多种 DoS 攻击方法进行防护，同时可以防止连接耗尽，对典型“以小吃大”的资源比拼型攻击(包括大规模的多线程下载)具有良好的防护能力。这种产品已经获得了市场的认可。早在正式发布之前，黑洞百兆、千兆两个型号的产品已经分别在若干家大型网络服务商、金融证券机构和教育网骨干节点进行了实际测试，分别可以很好的对百兆和千兆环境下大规模分布式拒绝攻击进行有效防护，“深受客户的好评”。甚至有的用户，仅仅经过了一些试用，在产品还没有正式下线发布的时候，就揣着支票等着提货。

不过，绿盟也深知阻击 DoS 的战斗才刚刚开始。“拒绝服务攻击的根源在于网络服务的公开性和面向对象的不可确定性，以及服务提供方资源的有限性和可耗尽性，这些因素决定了当前环境下并没有一劳永逸的最终解决方案，黑洞的推出，尽管扭转了一直以来抗拒绝服务攻击方面攻胜于防的不利局面，但是攻与防的较量却不会因此而结束。”

下载五花八门千余邮件 美记者攻破萨达姆邮箱

《北京晨报》报道，美国一名记者近日偶然进入了属于伊拉克总统萨达姆侯赛因的一个电子邮箱，他下载了信箱内的 1000 多封电子邮件，其中包括一些美国公司提出要与伊拉克做生意的请求、记者的采访要求和一些国外人士的请战要求等。

这名“黑客”记者名叫布赖恩麦克威廉斯。10 月的一个晚上，他进入了服务器设在阿联酋迪拜的伊拉克官方网站 www.uRukLInk.net/IRaq，突发奇想地破译了萨达姆的邮箱。

麦克威廉斯看到邮件的发件时间在今年6月中旬到 8 月中旬之间，当时邮箱已满，这些信既没被打开过，也没有被回复。萨达姆本人是否看过邮箱中的信件不得而知。

邮件的内容五花八门。一个自称在海湾战争时期当过伞兵的美国人写信给萨达姆说，希望能再有机会把他“这个讽刺漫画中的领导人从地球上抹去”。与此相反，奥地利维也纳一个萨达姆的崇拜者则表示，如果美国攻打伊拉克，“你只要给我送张票，我就会到伊拉克来跟美国人干仗。我枪法相当准。我的请求可是认真的。”

向用户需求转型反病毒软件将有重大变革

使用的方便性已成为用户选购杀毒软件的一个重要标准。近日国内权威反病毒企业北京江民公司，利用全国近三十个区域的服务中心，对近万名电脑用户进行面对面问卷调查，调查结果表明，90%以上的用户将方便性列为了选择杀毒软件的一个重要因素。

网络病毒在传播速度、破坏性、隐蔽性等特征都较单机病毒突出，杀毒软件已成为电脑标配。一直以来杀毒软件都被看作为高科技产品，只有具备相关专业知识的用户才会使用。如最初的杀毒软件都是在DOS下进行病毒查杀，有新病毒出现时反病毒企业就在报纸上将病毒代码公布出来供用户手工添加，由于当时计算机的数量相对较少，使用者多为一些具备相关知识的专家级用户，因而手工添加病毒代码的方式很受他们欢迎。

随着计算机及网络的快速发展与普及，越来越多的普通消费者成了电脑消费的主流，电脑也由原来单纯的工作平台发展成了多媒体娱乐平台，普通用户大多电脑知识贫乏，他们更多的是利用电脑来上网、休闲、娱乐等，只懂一些简单的操作，因而功能设置复杂的反病毒软件常常令他们束手无策。用户需求的反

病毒软件是简单、易用、高效人性化的产品，一些繁杂的功能都在后台运行，即便是初级用户在产品安装完成之后也无需太多的操作，就可以对电脑形成安全有效的全方位保护。

江民反病毒专家刘杰指出，由于国内反病毒软件发展与国外相比相对较晚，产品的研发还是以实验室本位为核心，产品的设计思路与功能与新形势下的用户需求产生脱节。国内的一些反病毒软件发展初期在产品的功能及操作界面的设计上，大多借签了一些国外优秀产品的长处，赋于了杀毒软件以强大的功能，但由于国内用户对于病毒的防范意识，以及对于电脑的熟练程度要远远落后于经济发达国家，因而有些功能虽然很强大，但由于其设置及操作复杂不易掌握，无法适应国内用户的需求。

用户的需求是反病毒软件发展的强大动力，但目前国内一些反病毒企业对于用户需求，往往还停留在用户的主动反馈阶段，对于用户的实际需求没有一个全面的把握和认识，产品研发处于被动地位，因而反病毒软件由实验室本位向用户需求转型，已成为反病毒企业在产品研发思路上的个重要指导方向。据悉江民公司在对全国近万名用户需求调查之后，对反病毒软件的易用性方面做了重大变革，即将要推出 KV 杀

毒王 2003 打破了传统，在产品的易用性及人性化方面做了重大改进，将为普通的电脑用户提供了一款病毒防护无处不在的新一代电脑安全产品。

首届中国互联网大会将在上海召开

以“互联网的应用——呼唤创新”为主题的首届中国互联网大会暨展示会，即将于 11 月 25 日至 27 日在上海召开。

据介绍，这届大会是首次由互联网行业协会发起，在中国举办的行业层次最高、规模最大的互联网盛会。人们将通过这次大会了解并分析国际、国内互联网业的最新发展趋势；探讨加入世贸组织后中国互联网业所面对的机遇、挑战及应对策略；研讨网络技术的发展及应用；交流行业经营、管理的经验；推动信息网络服务业的发展；促进先进网络文化建设；建设一个健康、繁荣的中国互联网业。

由于这两年中国互联网增长速度减缓，因此探讨其如何保持健康发展、如何在应用上创新，并为互联网在中国的进一步发展指明方向，将是这次大会的主要目的。

据悉，大会将全方位探讨的议题有电子政务、电子商务、网络经营、东西部地区互联网建设、下一代互联网和 IPV6、宽带网建设和骨干网技术、无线和移

动互联网技术、中国电子口岸简介、网络与运行技术、网络与信息安全、行业政策和法律建设、网络文化建设与网络信息资源开发、互联网知识产权保护等。这些涉及到互联网应用、技术、管理、知识产权、网络安全和互联网健康发展的全新议题，将呈现出层次高、视角新、范围广、应用强的显著特点。参与演讲的互联网专家、学者、企业界人士共有 100 位左右。

据介绍，同期举办的中国互联网展示会，将由国内顶级的互联网运营商、设备制造商、系统集成商、科研院所在占地 1000 平米的展厅里展示互联网的各种新技术、新设备、新产品、新业务和最新研究开发成果。

中国互联网协会理事长胡启恒说：“在这个互联网发展的重要关头，整个中国互联网行业的当务之急是要把握机遇、迎接挑战、找准中国互联网的增长点。”

大会由信息产业部批准，中国互联网协会主办，上海东浩服务贸易集团有限公司、上海现代国际展览有限公司、上海市互联网协会承办。

微软内部文件再次泄露 记载对付开放源码的策略

上周本站刊登了题为“微软:正在被 ”蚂蚁“蚕

食的巨人”的报道。非常巧合的是，就在这篇报道(日文)刊出的 11 月 8 日，一条名为“微软针对开放源码战略的内部文件被泄漏”的消息在全球不径而走。

开放源码业界团体 OSI(开放源码促进会)的创立者埃里克雷蒙德(ERIcS.Raymond)在 OSI 的 Web 站点(opensource.org)上刊登了这份微软的“内部文件”。

据称“内部文件”记录了微软在全世界进行的一项有关开放源码和 Linux 的调查结果。另外，还包括微软对该此前采取的战略为何效果适得其反的分析。其中“内部文件”指出在美国以外，尤其在德国、法国和日本，开放源码和 Linux 拥有众多的支持者，对于微软而言，这些市场将变得难以攻克。

雷蒙德公开微软的“内部文件”已经不是第一次了。1998 年他与此次一样，在网上登载了据称是消息灵通人士(没有公布这个人的姓名)那里得到文件，在开放源码阵营中激起了轩然大波，当时有人指出：“文件首次证明了微软已经千真万确地将开放源码看作了一种威胁”。另外，还有人认为：“微软对开放源码战略及其思考方式被暴露于光天化日之下”。

新“内部文件”的泄漏等于公开了微软的最新战略。这些文件是不是真的由微软内部泄漏的，目前不得而知，但可以肯定的是，刊登在 OSI 的 Web 站点上

的文件已经影响到了 IT 界。

被命名为“Halloween(万圣节)”的系列文件

雷蒙德公开文件此次是第 7 份，此次的文件被称为“HalloweenVII”。这一名称的来历是：1998 年 10 月底，雷蒙德表示得到了上面提到的第一份文件，在之后的一周里，他又表示得到了第二份文件。由于 10 月底是西方的万圣节，因此雷蒙德就将这些文件命名为“万圣节文件(HalloweenDocument)”，并给这些文件编了号。依次称为“HalloweenI”、“HalloweenII”和“HalloweenIII”等。

另外，雷蒙德还将他自己针对微软的声明等所做的批判、评论和讽刺文章整理成了三份文件，并予以公开。因此，万圣节文件此次已经是第 7 份了(注 1)。

注 1：“HalloweenI～III”和此次的“HalloweenVII”是以雷蒙德在微软的“内部文件”中加入注释的形式予以公开的。“HalloweenI～VI”则完全是雷蒙德自己写的作品。每份文件不但都加入了注释，而且还作为自己的作品公开，避免了侵权嫌疑。

记载着微软对付开放源码的策略

万圣节文件就是在这样的背景下一份一份地被

公开的。下面简单介绍一下其概要。首先介绍第一份“HalloweenⅠ”。在这份文件中，有关开放源码软件的描述是给微软及其产品和整个开发手段带来哪些影响。第二份“HalloweenⅡ”是微软针对 Linux 所做的技术分析。“HalloweenⅢ”记录的是微软对这些公开的万圣节文件所做的评论。

另外，以雷蒙德为首的开放源码阵营之所以异常关注这些文件，是因为在这些文件中明确地记录了微软“削弱开放源码软件势力”的对策。

这些文件中提到的对策包括：对付开放源码，使协议和应用程序非通用化；对付 Linux 则通过在 Linux 基础的通用协议和服务中嵌入扩展功能、制定新的协议，并由此改变软件业界的“游戏规则”。

另外，内部文件中还提到了如何使打算开发开放源码的开发者的兴趣转向微软产品的具体策略，比如进一步放宽 NT 源码的提供范围。也就是说，通过广泛地向教育机构和伙伴企业等公开源码，获得并行调试的优势。另外，通过低价或无偿提供入门级工具等，可以称之是微软对付开放源码的预防战略。

微软“内部文件”的曝光，使得人们更加明白微软到底是一家拥有何种思维方式的公司。雷蒙德曾把微软比喻成一个“处世精明与眼光狭隘共存的奇妙东

西”。

“日本对微软的共享源码持中立态度”

此次公开的“HalloweenVII”，据称微软曾于今年 9 月在德国柏林举办的战略会议上发表过。文件内容是被称为“AttItudesTowardsSharedSource&OpenSourceReseaRchPRoject(关于共享源码及开放源码研究计划的意见)”的调查项目的结果及其分析。也就是说，这份文件是一份调查报告书，目的是研究人们如何看待微软的源代码公开计划“共享源码”和开放源码。

文件表示此次调查以电话提问方式进行。以企业、教育及政府机构的 IT 负责人及决策者为对象、自 2001 年 7 月底至 9 月于美国、巴西、法国、德国和瑞典进行。

调查结果显示，开放源码目前已经在世界范围内被人们所接受，普遍认为开放源码的 TCO(总拥有成本)较低，这些优点引起了人们的关注。另外，就像本文开始所描述的那样，此次调查还显示，在德国、法国和日本有很多开放源码和 Linux 的支持者。有关日本的内容如下。

“日本人非常了解开放源码软件‘OSS’和 Linux 的情况，而且还对此抱有好感。该地区正在导入

Linux，而且人们还认为 Linux 具有比专用软件(软件开发商利用独自技术开发的软件)更低的 TCO。绝大多数日本回答者听说过有关共享源码的一些情况。而且这部分人群中的大部分人对共享源码持中立态度。另外，大多数人认为共享源码的优点同等或低于 OSS"。

另外，这份文件还写道，对 OSS、Linux、GPL(GNU 通用公共许可：开放源码的授权方式)进行批评非但没有给微软带来任何好处，甚至有时还会造成适得其反的效果。最后得出的结论是，指责 Linux 存在侵犯专利问题的可能性以及开放源码软件的开发手段缺乏解释责任并非上策。

雷蒙德的分析及对策

那么，对于此次的 HalloweenVII，雷蒙德又是如何理解的呢？看过其注释后，就会明白他总的来说比较满意。比如"过去 5 年来我们所倡导的内容以及所采取的战略都收到了成效。另外，即便在 TCO 的高低方面，我们也取得了胜利，给人们留下了深刻印象。并由此可以知道微软的信息操纵战略根本没有任何效果"。

他同时还暗示开放源码阵营也并不能高枕无忧、无所事事。因为他认为微软今后将会根据此次的调查结果重新采取新的战略。同时，雷蒙德提出了如下警

告：

“今后将会继续关注 TCO 的问题。就像 HalloweenVII 中所提出的那样，如果微软行动的话，它可以用尽手中的资金和权力，让现状来个彻底改变”(雷蒙德)。另外，作为其对策，雷蒙德说最有效的方法就是采取如下的做法：“用户必须密切注意微软的授权情况。我们需要做的是在产品上注明所需的时间和人工费”。

系列文件的泄漏是微软自编自演?

对于这一连串的万圣节文件，有人怀疑是不是微软故意泄漏的。比如，1998 年美国一媒体上就认为：“此事是不是微软为了向美国司法部和全世界表明该公司并非垄断性企业而故意泄漏的？”。也就是说，如果站在微软的立场来分析，情况并不是那么好。向外界表明正在受到 Linux、Apache 和 MozILLa 等开放源码阵营激烈竞争而处境异常艰难的微软的“弱小”，更有利于为该公司在反垄断诉讼带来有利影响。

但是，对此雷蒙德已断然否认。因为故意泄漏这些文件对微软来说太危险。“出示协议和服务的非通用化以及将开放源码产品排斥于市场以外等内容的文件将会成为该公司违反反垄断法的证据”(雷蒙德)。

如果从此次文件泄漏的时间和背景来考虑的话，只能说这里面的情况显得有点“微妙”。因为微软目前仍旧官司缠身，比如，与网景等竞争企业之间的诉讼、在欧洲的反垄断诉讼，以及来自个人的民事诉讼等。

不过，雷蒙德从文件中解读到的“为了彻底改变人们对微软产品 TCO 的认识，微软将采取信息操纵战略”也许是正确的。因此从从微软最近的行动来看，也的确如此。

南阳信息港被黑案告破 网站职工泄密码

河南省南阳市公安局近日运用科技手段，成功侦破了河南省首起攻击信息港的“黑客”犯罪案件。犯罪嫌疑人马某被依法刑事拘留。

据中国青年报报道，11 月 8 日上午 9 时，南阳市公安局接到南阳信息港报案称：11 月 7 日晚发现该市淅川信息港主页不能打开，被人进行攻击破坏，直接影响了十六大信息在网上的正常传播，要求迅速破案。

接到报警后，南阳市公安局迅速派出侦破小组，赶赴南阳信息港开展工作。经查，发现南阳信息港县级服务器被人非法入侵，并安装了管理工具。入侵者对信息港进行远程控制，从而达到破坏网站的目的。

侦技人员当日 9：48 时发现一个账号为“XYX”的非法用户正在登录该服务器。继而查明该账号的使用者为河南省邓州市的一个宽带专线用户。办案人员迅速赶赴邓州市，在当地公安、电信等部门的大力配合下，很快查清该用户是邓州市大西关街的马某某，使用电脑的是其儿子马某(2002 年 9 月进入河南中原职业技术学院学习信息工程专业，因违反校纪于 10 月 25 日被勒令退学)。

专案民警检查马某使用的电脑后，获取了其非法入侵信息港的犯罪证据，当场对马某依法进行传唤。经突审，马某对其非法入侵南阳信息港的犯罪事实供认不讳。

原来，马某在去年 7 月份上网聊天时认识了邓州信息港职工王某，王某擅自将自己掌握使用的密码透露给马某。马某在南阳信息港服务器中建立了名为“XYX”(逍遥仙)的超级账号，取得了对南阳信息港服务器的操作权限，随后多次登录实施攻击。

在“黑客”被抓获的当日，南阳信息港即恢复正常运行。涉案的邓州信息港职工王某被移交当地公安机关处理。

系统遭“黑客”袭击中国排协做最坏打算

日前，中国排球协会的技术统计系统突然遭遇

“黑客”袭击，导致比赛结果及技术排行榜陷于瘫痪。不过，排协正在全力“抢险”，比赛结果查询部分已经恢复，球员技术排行榜目前正在进一步核对，预计两天内整套系统将恢复正常运行。

据中国体育报报道，11 月 17 日，2003 年步步高女排联赛第一轮结束当晚，中国排协的技术统计系统遭遇了“黑客”袭击。排协技术统计系统的开放性是造成此次黑客袭击的主要

原因。访客在查询的时候，系统的 IP 地址自动显示，给了黑客以可乘之机。据新浪网统计数据显示，17 日当晚有 1 万多人访问排协的技术统计系统。新浪网与排协技术部正根据这 1 万多访客的 IP 地址进行排查，以追踪到袭击的黑客，并将保留追究其责任的权利。

排协技术部官员魏胜凡介绍说，排球联赛前几年影响力不是很大，造访排协技术统计系统的人员不多，因此他们对查询权限没有过多限制。新赛季第一轮即遭袭击，一方面表明联赛受关注程度逐步提高，另一方面也给排协敲响了安全警钟。排协正在考虑削减访客的权限，给 24 家俱乐部技术统计人员设置单独密码，一旦有疑问，他们可以随时与排协沟通并进行更正，确定所有数据准确无误后，再上传至供访客

查询的界面上，并且系统服务器的 IP 地址也将被隐藏。

为确保万无一失，排协做好遭遇黑客袭击最坏打算，每一轮、每一局的所有数据均保留有备份，另外还有各俱乐部的数据传真，一旦遭遇黑客袭击，排协能够在几分钟内用备份进行覆盖，恢复系统运行，以不影响媒体及访客的正常查询。

警方监视权扩大 美国批准电子侦察法案

美国一个联邦法庭星期一批准了一项扩大警方侦察权的议案，该议案授予警方监视互联网的使用、记录点击次数以及对恐怖主义和间谍嫌疑犯采取其它监视手段的权力。

外国情报监视复审法庭出人意料地以几乎全票通过推翻了某一低等法院的判决，并称司法部长阿什克罗夫特对新权力的要求是合理的。

这份 56 页的判决书为联邦特工扫清了根据 1978 外国情报监视法案(FISA)进行监视的法律程序上的障碍。

该法案作为后水门时代改革的一部分，允许进行大规模电子监视、电话窃听，以及秘密搜查住宅与办公场所。

爱国法案还修改了 FISA 监视的必要条件，认为

间谍或恐怖主义活动不应是调查的主要目的，而应是一个“重要目的”。

民间自由主义者组织表示，他们对此判决感到震惊，出于安全方面的考虑，该裁决的公开版被删改了。

联合国预测今年全球网民将占世界人口 1/10

尽管全球经济不景气，世界上的互联网用户人数仍在上升，预计 2002 年的该增长率接近 30%。

据英国广播公司消息，联合国贸易和发展会议预测，全球网民数量将在今年达到 6 亿 5 千 5 百万，这占世界人口的十分之一，而该数字在去年为 5 亿人。

该机构的年度电子商务和发展报告估计，互联网上进行交易的贸易额今年将达 23 亿美元，比去年增长了 50%，而该数字在 2003 年末可能会达到 39 亿美元。

报告说，2001 年新增的互联网用户中有三分之一来自发展中国家，但发达国家人口的上网率仍远高于发展中国家。

美国的网民人数最多，近 1.43 亿人；其次是中国，人数为 5660 万。英国有 40%的人上网，人数增长率为 33%。

2001 年，网民数量增长率在亚洲为 44%，在非洲是 43%，在拉丁美洲是 33%，在欧洲为 33%，在北美洲

为 10%。

非洲的网民人数在去年达到 670 万人，占人口比例的 1/118。

联合国贸易和发展会议的报告说，全球电子商务势头良好，但企业之间的电子商务在发展中国家并没有得到发展。

美国占有全球电子商务收入的 45%，西欧占有 25%，日本占有 15%，发展中国家则只占有 6.7%，而且主要是在亚太地区，其它发展中国家占有的比例仅为 1%。

这份报告还说，信息技术产品在发展中国家出口中的比例已超过农产品、纺织物和服装的比例总和，这主要是因为跨国公司利用了这些国家的廉价劳动力。

布什顾问：技术产业复苏将落后于经济复苏

美国总统经济顾问周三向 Comdex 的观众提供了他对技术产业未来的清醒分析，观众们从他的分析中得到了一次经济学的 101 课程教育。

布什总统经济政策特别助理 CaRLos BonILLa 说，1990 年代晚期公司在技术方面的过度投资意味着这样一个事实：即便美国经济确实复苏了，技术开支仍然有可能滞后。他是在 Comdex2002 秋季展示会上说

这番话的，他承认，美国经济已经咽下了 1990 年代后期的苦果。

BonILLa 是全美经济理事会的成员。他指出，告诉人们他们将看到被贬低的预期是一件困难的事，部分原因是人们刚刚开始回到地面和理解泡沫就是如此。

BonILLa 用图表和曲线阐释他的观点，对这些东西许多观众是第一次经历。图表显示在制造业和其他领域的持续衰退中，消费者开支是一个孤立的亮点。这表明经济复苏已经放缓并且受到阻碍。

他指出，显而易见，这表明经济走出衰退的时间要比其他任何模式都更加缓慢。

关于许多技术公司所关心的制造业延长的衰退，BonILLa 说，这是因为制造业要采用技术产业所生产的许多产品。在以后的会议基调演说中，他又说，你们要做的工作与那些使用你们产品的公司有着极大的不同。

BonILLa 说，在过去的泡沫时期，过度开支的规模在各个产业之间是不同的。十年间光纤业增长了许多，出现了许多新企业、工厂和设备，结果是许多公司并没有急迫的需要来采用和更换新设备。

微软公司将变更安全漏洞严重程度的评级方法

日本微软从 11 月 19 日开始改变了由公司公布的“安全信息”严重程度的评级方法。以往“安全信息”划分为“高（HIgh）”、“中（ModeRate）”以及“低（Low）”3 个等级，今后将改为“紧急（CRItIcaL）”、“重要（Important）”、“警告（ModeRate）”以及“注意（Low）”4 个等级。

此外，以往针对每个系统环境（“因特网服务器”、“企业内部网络服务器”以及“客户系统”）评价严重程度，今后将停止这一做法。这就是说，针对同一个安全漏洞将只设定一个严重程度。另外，美国微软于美国时间 11 月 18 日公布了此次变更评级方法。

据该公司公布的“经常收到的提问”内容，此次之所以变更为上述 4 个等级，是因为在过去的分级方法中，存在着由于像红色代码及 NImda 病毒等有可能被恶意利用的极端严重的安全漏洞与其他众多的安全性漏洞一样被评为“高”，无法明确反映它们之间的区别等问题。在新的评级方法中，前者被定为“紧急”，而后者多数情况下将被定为“重要”。

另外，由于事实上有很多系统可以被划分为几种不同的环境（例如，既是因特网服务器同时又属于企

业内部网络服务器系统），因此为了避免用户判断时出现混乱，该公司表示停止按系统环境进行评级的做法。

该公司表示，对于被评为“紧急”或“重要”的安全性漏洞，需要安装升级包（修正程序），尤其是对于“紧急”安全性漏洞更需要立即安装。

关于“警告”或“注意”类安全性漏洞则应该在阅读安全性信息以后判断该安全性漏洞是否对于该系统产生影响。在此基础上，确认升级包不会影响到系统之后才可以采用并安装。

几乎所有的用户都不会受到影响的安全性漏洞将被评级为“注意”级。不过由于这并不意味着完全不会受到影响，因此需要与“警告”或“注意”一样，在阅读安全性信息以后，根据需要与否来决定是否采用该升级包。

专家心目中的下一代互联网

无论在技术上还是在发展速度上，互联网在 20 世纪获得了巨大成功是世人公认的一个事实。即便在发展过程中产生了泡沫，目前正处在“挤水分、排泡沫”的调整阶段中，互联网及其应用仍在不断改变我们的工作方式和生活方式。未来的应用将使互联网对用户的价值变得更大，但绝非目前的互联网所能承接

和适应的。换言之，对于未来，我们呼唤新的互联网，即下一代互联网来满足需求。最早由官方提出下一代互联网计划的是美国克林顿政府于 1997 年 10 月 10 日出资 1 亿美元的 NGI 行动计划。其目的是研究下一代先进的组网技术，建立试验床和开发革命性应用。早在 1996 年 10 月 1 日由美国 34 所著名大学在芝加哥发起的一个用于科研、教学的第 2 代互联网项目(Internet2，简称 I2)后来也并入 NGI 计划。

然而，到了 90 年代末，电信市场在世界范围内开放竞争，互联网的广泛使用使数据业务急剧增长，用户对多媒体业务产生了强烈需求，用户对移动性的需求与日俱增。电信业面临着强烈的市场冲击与技术冲击。在这种形势下，出现了下一代网络(NGN)的提法，并成为大家讨论最多的一个话题。NGN 是网络界为了描述未来电信网共同使用的一个新概念。实际上它涉及了下一代核心网、城域网、接入网、移动网、用户驻地网等。但时至今日，运营商、制造商和服务提供商对 NGN 仍看法各异。现在大家都希望能够对 NGN 取得共识，好对它制定国际标准。因此，ITUT 在 2002 年 1 月的 13 组会议上决定启动 NGN 的标准化工作，在第 13 研究组内建立一个新的项目，叫 NGN 2004 PRoject。该项目将与 ITUT 已有的 GII 项目相对应，

因为 ITUT 把 NGN 看作是 GII 的具体实现。ITU 在 1995 年启动的GII项目形成了目前的Y系列建议，包括GII原则与架构、GII 场景设想方法与举例、信息通信结构、互连参考模型，后来又加入了有关 IP 传送的内容。但在 Y 系列建议中除了互操作与互通问题没有完备外，网络上如何具体实现的问题更是空白。NGN 2004 PRoject 的目标即是填补这一空白，并在 2004 年制定出相关建议。对于 NGN，ITU 至今尚未给出定义，只有欧洲ETSI的NGN启动小组在其报告中曾建议把NGN定义为：NGN 是定义和部署网络的一个概念，由于它们形式上分为不同的层面和使用开放的接口，所以 NGN 给服务提供商与运营商提供了一个能逐步演进的平台，不断创造、开放和管理新的服务。

从一个电信工程师的角度看，在三网融合的趋势下，下一代互联网在许多地方与上面所说的 NGN 是共同的。

互联网面临的挑战

互联网在走到 21 世纪开元之年时忽然发现由它带动起来的网络经济被过多的泡沫所覆盖，变得举步维艰了。它在前进的道路上面临着一系列的挑战。

挑战之一：为了让人们创造更多更有价值的服务与应用，互联网需要提供比现在大得多的通信能力，

很可能所需的接入带宽要比目前大 100 倍，骨干网的总带宽要比目前大 1000 倍。故如何创造既满足上述通信能力，产生很大规模经济，在总成本上又只需作适度增加的新技术就是一大挑战。

挑战之二：今天的互联网所提供的服务是“尽力而为”的，得不到质量保证，这显然是不能令人满意的，尤其是对那些实时性要求严格的服务。“尽力而为”也使运营商或服务提供商难以推出能盈利的商业模式，妨碍互联网的深入发展。故如何从“尽力而为”的服务过渡到具有服务质量保证的强势服务又是一大挑战。

挑战之三：1998 年美国首次用数字鸿沟来比喻信息贫富差距。在过去的 40 多年中，全球的电信网络以每年 4%～7%的速度稳步发展，网络规模增长了 8 倍多。不同国家之间电话普及率的差距一直在不断缩小。然而，当我们正在弥补 80 年代的电话鸿沟时，90 年代的信息革命浪潮又形成了新的更大的鸿沟。截至 2001 年 1 月，占世界人口 15%的高收入者占有了全球固定电话线数的 55%、移动用户数的 65%、互联网用户数的 74%。其中互联网鸿沟尤其大。不仅发展中国家与发达国家之间存在明显的数字鸿沟，而且每个国家内部，发达地区和贫困地区之间、城市和农村之

间、富人和穷人之间、不同种族之间也存在着较大的信息贫富差距。所以，缩小数字鸿沟，实现互联网普遍服务，向全人类普及互联网接入与应用是我们面临的另一个巨大挑战。

挑战之四：90 年代互联网以惊人的速度发展着，到 2002 年初全球用户数已超过 5 亿。今后随着政府上网、企业上网、个人上网、汽车上网、设备上网、家电上网等等，现有互联网协议 IPv4 定义的有限地址空间很快就要不够用，估计在 2005—2010 年间将分配完毕(而且 70%的 IP 地址为美国占有)。这势必妨碍互联网的普及和深入发展。为了扩大地址空间，需要用下一代的互联网协议 IPv6 来重新定义地址空间。从 IPv4 向 IPv6 的过渡不仅需要大量投资，而且还要保证平滑过渡，这也是一个不小的挑战。

挑战之五：互联网自 90 年代中期商用化以来很快形成了所谓的眼球经济，即以冲浪、浏览为主的单一商业模式。虽然发展很快，但是没有形成多赢的新的价值链以及相应的商业模式。互联网要在完全开放与竞争的市场环境中得以持续发展，不走入死胡同，就必须从眼球经济走向能够创收、盈利的模式。如何在互联网上推出更多更有价值并能不断衍生的服务与应用，如何形成新的价值链和找出能够盈利的商业

模式都是必须面对的挑战。

对下一代互联网的基本要求

为了迎接上述挑战，更好地为未来服务，下一代互联网至少要满足下列基本要求：

为了支持更多更有价值的服务与应用，特别是支持今后将成为主要市场驱动力的视像应用，下一代互联网应是一个具有巨大容量、在每一个网络环节都不会产生带宽瓶颈的网络；

为了消灭地址壁垒，恢复因地址有限而失去的端到端连接功能，让数十、上百亿的人和设备上网，实现互联网的普遍服务，并且把服务方式由提取(puLL)演进为推送(push)，下一代互联网应是一个具有海量地址空间、能实现端到端连接的网络。估计在 7—10 年内，一个用户将掌管平均 10 个地址，将来还要多；

面对用户对新服务之需求的急剧增长，下一代互联网应是一个基于 IP 的能够承载话音、多媒体、数据和视像等所有比特流的多业务网，并能通过各种各样的传送特性(实时与非实时、由低到高的数据速率、不同的 QoS、点到点/多播/广播/会话/会议等等)来满足这些业务，使服务质量得到保证，令用户满意，运营商可以实现优质优价；

为了适应完全开放与竞争的环境，让众多的运营

商、制造商和服务提供商方便地进入市场参与竞争，易于生成和运行各种服务，下一代互联网的网络结构和功能组织应当提供开放式的接口；

服务与应用是无止境的，为了让服务与应用能够不断演进，而不受制于网络，下一代互联网应是一个在与网络传送层及接入层分开的服务平台上提供服务与应用的网络，也就是说，服务的提供要与网络分开，服务功能要与传送功能分开；

为了充分挖掘现有网络设施潜力和保护已有投资，下一代互联网应是一个具有后向兼容性、能与传统网络(PSTN、IPv4 网等)互操作与互通、允许平滑演进的网络；

移动电话的大发展充分说明人类对移动性的旺盛需求，电话服务需要移动性，互联网服务同样需要移动性，现在越来越多的人希望在移动的过程中高速接入互联网，获取急需的信息，完成所想做的事情。下一代互联网应能支持普遍的移动性和游牧性。

支撑下一代互联网的主要技术

为了满足上述基本要求，下一代互联网必须得到许多新技术的支持。下面列举若干比较主要的技术。

1.IPv6

下一代互联网将是基于 IPv6 的网络。IPv6 的提

出最初是为了扩大 IP 地址空间。实际上，IPv4 除了在地址空间方面有很大的局限性，成为互联网发展的最大障碍外，IPv4 在服务质量、传送速度、安全性、支持移动性和多播等方面也存在着局限性，这些局限性同样妨碍着互联网的进一步发展，使许多服务与应用难以在互联网上开展。因此，在 IPv6 的设计过程中除了一劳永逸地解决了地址短缺问题以外，还考虑了在 IPv4 中解决不好的其它问题。IPv6 相对于 IPv4 的主要优势是：扩大了地址空间，提高了网络的整体吞吐量，服务质量得到很大改善，安全性有了更好的保证，支持即插即用和移动性，更好地实现了多播功能。IPv6 实际上改变了互联网的核心，需要开发新的大型路由器，使目前的互联网变成一个性能更高、成本更低的全球互联网，彻底结束拨号上网时代。当然，要实现这一目标并非易事，让 IPv6 一步取代 IPv4 既不可能也无必要，过渡将是长期的，即便采取平滑的过渡策略，成本也是高的，困难和问题必定存在。但从长远看，改变后会引入许多新的服务与应用，使互联网转向新的能盈利的商业模式，将更有利于互联网的持续长久发展。

2.光纤高速传输技术

下一代互联网需要更高的速率、更大的容量，但

到目前为止我们能够看到的，并能实现的最理想的传送媒介仍然是光。因为只有利用光谱才能带给我们充裕的带宽。光纤高速传输技术现正沿着扩大单一波长传输容量、超长距离传输和密集波分复用(DWDM)系统三个方向在发展。单一波长传输容量已做到40GBit/s，超长距离实现了1.28TBit/s(128x10G)无再生传送8000公里，波分复用实验室最高水平已做到273个波长、每波长40GBit的10.9TBit系统(日本NEC)。单一光纤的传输容量自1980到2000年这20年里增加了大约1万倍(见表1)。预计几年后单纤容量将再增加16倍，达到6.4TBit/s。再往后，人们的目标是使单纤容量达到1Bit/s/Hz的光谱效率。一条光纤的可用带宽约为30—50THz，故目前的光谱效率才0.1Bit/s/Hz。

3.光交换与智能光网

下一代互联网需要更加灵活、更加有效的光传送网。组网技术现正从具有分插复用和交叉连接功能的光联网向利用光交换机构成的智能光网发展，从环形网向网状网发展，从光电光交换向全光交换发展。智能光网能在容量灵活性、成本有效性、网络可扩展性、业务提供灵活性、用户自助性、覆盖性和可靠性等方面比点到点传输系统和光联网带来更多的好处。2001

年光交换机开始越来越多地从实验室走向有限的商用生产，开始在网络边缘和网络核心使用。采用微电机械系统(MEMS)技术的全光交换机取得较大进展。朗讯的256×256全光波长路由器WaveStaRLambdaRouteR已经投入商用。XRos的光交换机X1000能支持1152个端口，达到电信级的最低要求。AcceLIghtNetworksInc.和NTT展示了基于通用MPLS(GMPLS)的大型太比特全光交换机。

4.宽带接入

下一代互联网必须要有宽带接入技术的支持，因为只有接入网的带宽瓶颈被打开，各种宽带服务与应用才能开展起来，网络容量的潜力才能真正发挥。在这方面有三个技术要提一下。一是甚高速数字用户线路(VDSL)；二是基于以太网无源光网(EPON)的光纤到家(FTTH)；三是自由空间光系统(FSO)。

与ADSL相比，VDSL既可工作于不对称方式，也可工作于对称方式，速度要快得多，能支持ADSL不能支持的业务。以不对称方式工作，VDSL的下行速率可高达52MBit/s；以对称方式工作，速率可达26MBit/s。再加上VDSL不基于ATM技术、设备简单、建设快，故总体造价比ADSL便宜。由于具有上述优势，VDSL在2001年开始升温。特别是利用FTTC或

FTTB 配合 VDSL 可以成为一种很好的宽带接入方案，既能满足目前需要，也能适应将来更新的技术。采用离散多音(DMT)方式的 VDSL 标准取得了较大进展，在世界 5 个地方演示了 DMTVDSL，成功地实现了高速互联网接入和高质量视像传送，包括会议电视、广播电视、VOD。

所谓 EPON 就是把全部数据装在以太网帧内来传送的一种 PON。考虑到现在 95%的 LAN 都使用以太网，把以太网技术用于对 IP 数据最优的接入网是十分合乎逻辑的。由 EPON 支持的 FTTH 现正在悄然兴起，它能支持千兆比特的速率，而且成本不久可降到与 DSL 和 HFC 网相当。美国在 FTTH 安装方面在过去 12 个月中增加了 200%多。

FSO 是光纤通信与无线通信的结合。它通过大气而不是光纤传送光信号。FSO 技术既能提供类似光纤的速率，在无线接入带宽上有了明显突破，又不需在频谱这样的稀有资源方面有很大的初始投资(因为无需许可证)。与光纤线路相比，FSO 系统不仅安装时间少得多，成本也低得多，FSO 已经在企业和多住户单元(MDU)市场得到使用。

5.城域网

城域网也是下一代互联网中不可忽视的一部分。

城域网的解决方案十分活跃，有基于 SONET/SDH/SDH 的、基于 ATM 的、也有基于以太网或 WDM 的，以及 MPLS 和弹性分组环技术(RPR)等。这里需要一提的是 RPR 和城域光网(MON)，它们是城域网在 2001 年的两个主要成就。弹性分组环是面向数据(特别是以太网)的一种光环新技术，它利用了大部分数据业务的实时性不如话音那样强的事实，使用双环工作的方式。RPR 与媒体无关，可扩展，采用分布式的管理、拥塞控制与保护机制，具备分服务等级的能力。它能比 SONET/SDH 更有效地分配带宽和处理数据，从而降低运营商及其企业客户的成本，使运营商在城域网内通过以太网运行电信级的业务成为可能。城域光网是另一代表发展方向的城域网技术，其目的是把光网在成本与网络效率方面的好处带给最终用户。城域光网是一个扩展性非常好并能适应未来的透明、灵活、可靠的多业务平台，能提供动态的、基于标准的多协议支持，同时具备高效配置、生存能力和综合网络管理的能力。AT&amp；T 在 2001 年 1 月底推出城域光网业务，业务名称为超可靠宽带网(ULtRavaILabLeBRoadband Network)，网络跨度达到 25 英里，用户可以选择最高到 2.5GBit/s 的多种带宽。此外，还提供 SLA 服务质量保证，网络保证 99.999%可用性(即每年的故障时

间不超过 5 分钟)。

6.软交换

为了把控制功能(包括服务控制功能和网络资源控制功能)与传送功能完全分开，下一代互联网需要使用软交换技术。软交换的概念基于新的网络功能模型分层(分为接入与传送层、媒体层、控制层与网络服务层四层)概念，从而对各种功能作不同程度的集成，把它们分离开来，通过各种接口协议，使业务提供者可以非常灵活地将业务传送和控制协议结合起来，实现业务融合和业务转移，非常适用于不同网络并存互通的需要，也适用于从话音网向多业务多媒体网的演进。ITU 和 IETF 联合批准的媒体网关控制器(MGC)和媒体网关(MG)之间的接口协议 H.248/Megaco 是一个关键的协议，标志着电信界与互联网界为推进下一代网而作出的一次重大努力。

7.3G 和后 3G 移动通信系统

3G 基于多媒体 IP 业务，传输容量更大，灵活性更高，形成了家族式的世界单一标准，并将引入新的商业模式，目前正处在走向大规模商用的关键时刻。包括 4G 在内的后 3G 系统将基于宽带多媒体业务，使用更高的频带，使传输容量再上一个台阶。在不同网络间可无缝提供服务，网络可以自行组织，终端可以

重新配置和随身佩带，是一个包括卫星通信在内的端到端 IP 系统，与其它技术共享一个 IP 核心网。它们都是支持下一代移动互联网的基础设施。

ITU 以及一些发达国家都开展了关于后 3G 移动通信系统(包括 4G)的工作。主要沿着三个方向。第一是 3G 标准 WCDMA 的进一步演进。演进的方向有两个：高速下行链路分组数据接入(HSDPA)和业务协商。HSDPA 的主要目标是允许 WCDMA 对“尽力”分组数据业务支持大约 8~10MBit/s 的下行链路峰值数据速率；业务协商将允许对 QoS 参数进行协商，以便对 QoS 的控制有更大的灵活性。第二是欧洲提出的一种旨在提供宽带传输能力的过渡系统，叫移动宽带系统(MBS)，其最高速率可达 150MBit/s。第三是对 4G 的研究，当前开展的主要是概念与框架的研究，着重于需求分析、性能分析和关键技术的分析。2001 年在特别网(采用分布式操作、动态网络拓扑、波动链路容量和低功率设备、通信距离一般在 10 米半径以内的网络)、多跳技术(旨在扩大覆盖范围)、移动性(快速有效的位置登记管理)、高效率切换和调制技术等方面开展较多研究。

8.IP 终端

随着互联网的普及及其端到端连接功能的恢复，

越来越多的用户想把 IP 接入家里。企业内联网的使用越来越普遍，也驱动着对基于 IP 的应用的需求。这一切都意味着需要越来越多基于 IP 的设备联网。许多公司现正在从固定电话机开始开发基于 IP 的用户设备，包括汽车的仪表板、建筑物的空调系统以及家用电器，从音响设备和电冰箱到调光开关和电咖啡壶。所有这些设备都将挂在网上，可以在家庭 LAN 或个人域网(PAN)的 PC 机上接入或从远端 PC 机接入。

经过高速发展后的互联网，其核心地位已不可撼动，但在它迈向下一步的时候遇到了重大的挑战。时代在呼唤下一代互联网。下一代互联网最终将以新的面貌出现在地平线上，它将在容量(包括带宽与地址)和质量上给予我们足够的保证，逐渐与电信网融合在一起，让我们可以放开手脚创造更多更有价值的服务与应用，把人类带入信息时代。

信息安全：与危险同行

据社会学家考察，早在远古时代，人类的祖先就已表现出对风险的深深困惑和对其奥秘的孜孜探究，其最发人深思而又最饶有趣味的例子，莫过于“轮子”和“骰子”的相伴而行。科技史专家公认，“轮子”是自“钻木取火”后

人类最伟大的发明，考古发掘已经从墓葬中发现

了距今 5500 年以前的用于运输重物的轮子，以后的纺轮、齿轮、涡轮无不是这一伟大发明的模仿和延伸，可以说人类的早期文明就是借助于火与轮生长起来的。然而，几乎与“轮子”的发明同步，另一种“滚动物”——“骰子”也应运而生，而按《大英百科全书》的解释，骰子最初的功能就是占卜，原始人以之预测凶吉，以后才用于赌博。

这是不是可以说明，人类对自己的行为的风险意识是与生俱来的？在人的潜意识里，未知与风险的刺激并不弱于发明和劳作？并且，越是重大的发明，越是有重大价值的行为，也越是风险莫测？

信息技术的发明和发展，正在以最现代的形态演绎着这一最古老的定则。

10 月底在常州召开的第 17 次全国计算机安全学术交流会暨电子政务安全讨论会上，国家计算机网络与信息安全管理中心副主任兼总工程师方滨兴演示的幻灯片让在场的 140 位与会者心惊肉跳：今年 10 月上半月，全球仅黑客攻击事件就发生了 7228 次之多，这还不算肆意泛滥的病毒，莫明其妙的系统崩溃，以及防不胜防的来自地面和空中的窃密者；今年 1 至 3 月，观察到的全球病毒扩散次数超过 5.8 亿次，中国大陆一则发出的扩散次数超过 3.13 亿次，全球有

33.6 万个 IP 被感染，中国大陆超过 8.89 万个。而据介绍，国外最新研制出的计算机“接收还原设备”，可以在数百米、甚至数公里的距离内接收任何一台未采取保护措施的计算机屏幕信息。

信息安全产业的“繁荣”则提供了另一个佐证。1997 年以来，我国 GDP 的年增长率约为 8%，信息产业的增长约为 30%，信息安全市场的增长率却超过了 50%。其中，1999 年安全产品约为 9 亿元人民币，2000 年超过 19 亿元，2001 年超过 40 亿，今年预计将达到 100 亿元！另据 IDC 公司提供的数据，2001 年全球信息安全产品市场已高达 660 亿美元，到 2006 年，这个数字将增至 1550 亿美元。该公司对 1000 名 IT 经理人进行的调查表明，40%的经理人把 IT 安全列为最优先考虑的问题，多数人认为“安全是 IT 开支唯一要增加的领域”。

难怪信息安全企业近年来如雨后春笋（国内信息安全企业已由 2000 年的 300 家增长到现在的 1300 余家），也难怪信息安全市场会成为包括联想、瑞星、紫光、金山、东大阿尔派等在内的厂商们“鏖战”的新热土。

易思克网络安全技术公司总工程师邵通接受笔者采访时甚至断言：“下一轮计算机的换代将不是因

为速度，而是因为安全！”

正视“不安全文化”

然而，当人们静下心来思考信息安全的对策时可能会沮丧地发现，自己首先需要解决的问题似乎不是如何根除危险，而是如何“端正思想”，即如何“容忍”危险，学会“与危险共存”。因为从根上说，危险是不可能一劳永逸地解除的。

科学家早已告诫，人类智力的进步并不意味着风险的化解，因为这种进步会鼓励人们不断把触角伸向新的、风险莫测的领域。人们甚至发现，如果把已知的事物看作一个圆，圆周之外为未知之物的话，则“所知越多，圆周越长，与未知之物的接触面也就越大，从而遇到的风险也越多越频繁”。

在这个意义上，今人面临的风险并不弱于古人。古人固然享受不到计算机网络等新技术带来的方便、效率和财富，可也绝对不会遭遇核武器、生化武器、克隆人、网络战等可能带来的灾难和荒恐，更不会想到，“9.11”后“打开一封信都可能是一种致命的危险”。

于是人们便不无兴趣但又并不轻松地看到，当网络专家们兴奋地论证着“网络效应与结点的增多成正比”时，站在一旁的安全专家却忙不迭地告诫“网络

结点越多网络越脆弱”——多一个链接就多一分被黑客和病毒攻击的危险。

信息安全的话题在这儿似乎成了一个无解的悖论。一方面是人们忙忙碌碌地寻找着各种各样的网络解决方案，另一方面却是“连网本身就是最大的不安全”。有位反病毒专家在一个研讨会上发问“谁的电脑没有感染过病毒”？台下一百多号听众中竟没有举起一只手来。由此得出的结论只能有两个：其一，信息技术的发展与危险的发展如影随形，此长彼亦长；其二，如果有谁想追求“百分之百的安全”，办法只有一个，就是把自己关进信息孤岛。这显然是人们不愿意的。

信息安全专家、中国现代国际关系研究所信息与社会发展研究室主任俞晓秋曾忧心仲仲地谈到信息革命给现代社会带来的“脆弱性”问题。的确，当一个社会从经济到文化，从工作到生活，从军事到政务都已离不开信息技术，而信息技术又隐藏着巨大且不可能根除的风险时，这个社会的“脆弱性”也就无可怀疑了。现在面临的问题已不在于这种脆弱性的有无，而在于如何控制这种脆弱性，减少风险“发作”的次数和强度，把对信息安全的威胁降到社会可以接受的限度以内。

而信息系统的脆弱性涉及技术、应用、管理等多种因素，包括让你防不胜防的天灾人祸。即使你采用了世界上最好的安全产品，内部管理慎之又慎，也难保万一。遭遇“9.11”的一家美国公司为保证信息安全而斥巨资建立了数据备份中心，却毁于百密一疏之中——它把备份系统放到了世贸中心另一栋大楼里，想不到两栋大楼都在恐怖袭击中化为灰烬。

我们还知道，保障信息安全是以牺牲方便性、灵活性为代价的。如同你给家里装了一把很复杂的门锁，小偷是撬不开了，但你自己进门也麻烦了许多，忘记了密码还会把自己锁在门外。为信息安全的层层加密不仅会抬高成本，还会影响系统运行速度。通常情况下人在电脑屏幕前等待的耐心只有 7 秒钟，如果因为安全而降低了工作效率，不少人宁可放弃安全。著名社会学家、慕尼黑大学教授乌尔里希贝克就曾批评布什政府所主张的对恐怖分子的全面控制方针“显然是不可能的，而且最终可能导致失望，产生相反的结果”。

在这里，“不安全文化”成了解决信息安全首先需要正视的事实。乌尔里希贝克据此提出，当今社会应当“发展一种不安全文化”，在他看来，零风险如同零失业率一样，充其量不过是一种“集体的谎言”。

如果承认此话有些道理，那么我们的信息安全策略就须把“不安全文化”纳入其中，作为思考和应对信息安全问题的重要参考系。这其实也就是管理学所说的风险管理的思路。安全厂商常常会信誓旦旦地给用户作出“全面控制”、“万无一失”的保证。但这是不可能的，你也千万别信。

再深一步看，“不安全文化”还涉及人们承担风险的意识，而这也是发展和应用信息技术所必不可少的。期望一切都在理性的控制之内，期望绝对安全了再去投资或应用，所付出的代价会更大。著名经济学家凯恩思就曾说过，假如一个人生性不喜欢碰运气，而仅靠冷静盘算，恐怕不会有所作为。美国学者乔治吉尔德甚至认为，一个社会获得成功的主要秘密，也许在于它把追求安全转变为愿意冒险的能力。在这里，对危险的承认和控制，而不是对危险的一劳永逸地根除的意愿，构成了“不安全文化”的基础性内容。

信息安全的两个视角

由操作层面看，既然“不安全文化”视不安全为一种常态，对信息风险的防范理所当然地就应当纳入企业和社会日常管理的轨道。在第 17 次全国计算机安全学术交流会暨电子政务安全讨论会上，来自公安部、总参谋部、信息产业部、中科院等数十家单位的

140 多位专家、企业家和政府官员，就信息风险的防范深入交换了意见，归纳起来有两个大的视角：战略视角、经济视角。

在战略视角方面，中科院院士沈昌祥强调信息安全是一项包括技术层面、管理层面、法律层面的社会系统工程，延伸开来还应包括观念和文化层面，例如从文化意义上构建信息技术的行为准则，培育网络空间的道德规范。我国已经颁布了一系列有关信息安全的管理条例，但还缺少国家级的统领全局的信息安全框架，这不能不说是一个巨大的缺憾。他介绍，“911”后美国信息基础设施保护委员会（PCIPB）列出了 53 个信息安全重点问题，把信息安全列入国家战略。在这个战略中，信息安全保护被分成 5 个等级：第一级是家庭用户与小型商业机构，第二级是大型企业，第三级是高等教育、联邦政府、州与地方政府等关键部门，第四级是国家优先任务，第五级是全球性合作网络。五个等级五种保护模式，如第一级保护只要求采用密码、过滤、防病毒软件等技术，使用高速连接设备的还应考虑防火墙；第五级保护则包括建立广泛的“安全文化”，推动国际化合作网络的发展，在安全事件初露端倪时便能通过该网络进行确认并提供防护。

北方计算中心副主任贾颖禾认为，信息安全的战略规划不只是国家的事情，也是企业要做的事情，“首先要从安全评估和规划入手，不要一开始就进入技术细节”。任何信息安全保障体系的建立都大致经历评估、制订策略、系统设计、实施和调整的过程，并且这一过程还应当随信息安全的阶段性发展而反复，不能一劳永逸。与国家信息安全的战略规划一样，企业的信息安全规划也应当把信息的分级管理作为基础性内容，“第一件要做的事是把你的信息分分类，有的需要重点保护，有的只是一般的保护，必要时还应该分出等级，以便采取不同的保护措施”。制定规划要技术与管理并重，构筑由保护、检测、响应、恢复等环节组成的保障体系。

与战略视角相比，经济视角更为企业所关心。中国工程院院士、国家信息化专家咨询委员会副主任何德全就曾谈及解决信息安全的“经济学角度”，主张以此为基础解决好技术与管理两个问题。河北信息产业厅的石起伟说他们“只关心产业的事，就是信息化安全的产业化”，譬如 PKI（密钥认证平台）从商业上怎么能保证交易的安全，商业上的应用需要多大的成本，“投资不能超过 15%，如果投资大了，经济性没有了，这个技术肯定是不行的，企业不会要”。贾颖禾

也谈到了企业信息安全投入的比例问题：一般来说，没有特别的需要，为信息安全的投入不应超过总投资额的 15%，逐步增加为好，否则你只能卖给军队。军事学上已经提出了“五维空间（陆海空天电）”的概念，信息战不可避免地会成为未来军事斗争的主要样式之一，军队在信息保密方面可以不计成本。

经济视角还应导入信息风险的评估之中：评估要从自身情况出发，并非报章和书本上提到的所有威胁你都会遇到，威胁的程度也有很大的差别。通常情况下，越小的组织，越要多着眼于内部的问题；组织越大，分布越散，来自外部的威胁就越大，可能造成的损失也越大。网络脆弱性评估的专业性强，涉及网络连接方式、信息的产生、分布和使用状况，同时还涉及安全管理水平和人员素质，需借助专家和技术服务的力量。从“不安全文化”的眼光看，脆弱性客观地存在于任何系统中，经过努力可以减少却不可能完全消除。

专家们认为，这儿涉及的实际是个“适度防范”的问题，而“适度”的标准很大程度上又是由经济投入定盘子的（另一条标准是因加强信息安全而牺牲方便性和灵活性的限度）。在这一点上，经济视角与战略视角，特别是对信息分级保护的规划衔接起来了。

这就如同，居家过日子只需买一把好门锁或者加一个防盗门，企业的财会部门则必需有保险箱，如果是银行的金库，那就需要派卫兵把守了。上海宝信软件公司技术总监王柏青的结论是“我们需要的是适度的安全，对信息安全的授权要最小化”。贾颖禾说人们爱讲“木桶原理”，但在信息安全保护上，这个桶就有点过大了，而且“桶”还是用金子做的，很贵，所以必须划分边界，区别保护对象，把有限的资金放在最需要保护的地方。信息安全国家重点实验室主任冯登国更明确提出：以经费为杠杆，突出重点，“80%的信息安全经费要用在那 20%最需要保护的领域”。

光有盾是不行的

几乎整个 10 月份，美国人都是在恐惧中度过的——马里兰州和弗吉尼亚州先后有 10 人死于“连环枪手”射出的子弹，另有 3 人受伤。如果不是最终捉住了凶手，不知还会有多少人丧生，而凶手一旦“成功”，其“示范效应”可能带来的后果更会让人不寒而栗。

这意味着“与危险同行”仅有防范远远不够，更重要的是找到入侵者或疏于防范的责任人，让他们付出应有的代价，并以此警示后人。毛泽东早就谈及“积极防御”或曰“攻势防御”的问题，从战略上看，进

攻往往是最好的防御。

信息安全风险的防范尤其是这样。何德全院士谈及信息安全问题时强调，当前各国都面临着同样一个挑战，那就是“信息防御的成本越来越高，而攻击的成本则越来越低”，一个不知名的中学生制造的病毒就可以让成千上万台电脑陷入瘫痪。为此，信息安全的武器库中光有盾是不行的，还得有矛。

而纵观国内信息安全市场：商用密码、防火墙、防病毒、身份识别、网络隔离、可信服务、安全服务、备份恢复等等，主流产品几乎都是防御型的，这种格局应尽早改变。一个对风险责任人缺乏震慑力的防御体系必定是低效的，防御的成本也会越来越高，而当成本的增长超出了“经济视角”的承受力时，信息安全就将陷入空谈。

国家计算机网络防范中心首席科学家许榕生在介绍国际信息安全技术最新进展时说，国际信息安全技术已经从被动防范走向主动出击，当前最热门的“攻击型”技术有两项，一项是取证技术，另外一项是网络入侵陷阱技术。

取证技术是针对计算机入侵、犯罪进行证据获取、保存、分析和出示的技术。如同美国“连环杀手”会在射出的子弹中留下可供破案的痕迹一样，计算机

入侵者也会留下这样那样的痕迹，信息安全中的取证技术就是找出其中的蛛丝马迹进行分析取证。计算机在受到攻击后往往被安装了后门，删除了文件，取证机则可以利用文件系统的特征，结合相关工具，尽可能真实地恢复这些文件信息，从中发现鲜为人知的东西。

中科院国家信息安全重点实验室研究员赵战生谈及取证技术的意义时认为，信息安全管理，说到底就是“摘责任”，出了问题，需要先把责任搞搞清楚，之后才能采取下一步的措施。这样既可以找准薄弱环节，理顺管理，又能对罪犯起到震慑作用。而且，取证和捉住罪犯的目的不仅仅是为了找到证据，更是为了获知攻击行为的特征，研究反击技术，以便先发制人。

网络入侵陷阱技术类似于战场上的伪装技术，它采用网络重定向技术创建一个欺骗主机，该主机可以建立多个操作系统伪装环境（即陷阱），保护对应的服务器。通过对陷阱机的监视，还可以看到攻击者在做些什么。

在今年 6 月夏威夷召开的第 14 届事件响应与安全组织论坛上，这种主动出击的安全技术成为研讨热点，其中取证技术的论文多达 6 篇。

许榕生说中国人素以“龙”的传人自誉，其实龙是可以变色的，尤其是在信息安全手段方面应当道高一尺魔高一丈，随着犯罪手段的变化而变化。遗憾的是，目前在国内，大家谈来谈去仍然是防火墙、入侵检测这些传统技术。其实，用于网络隔离与过滤的防火墙仅仅类似于一个门岗，大多数入侵检测系统则类似于一种盗贼警报，都是被动式的防范，这还是国外五年前的水平。

出路在于“中国芯”？

据披露，在世界范围内，中国网络安全水平被排在等级最低的“第四类”，与某些非洲国家为伍，我们的邻居兼 IT 产业对手印度排在第三类。

谈及中国信息安全的“根本问题”或“最大隐患”时，业内人士多首选“核心技术缺乏”这一条。中国计算机安全专委会副秘书长、公安部计算机局原总工程师缪道期研究员说，中国信息安全有“三大黑洞”，一是用外国制造的芯片；二是用外国的操作系统和数据库管理系统；三是用外国的网管软件。“你用了外国的东西，万一发生战争，你不知道里头有些什么‘后门’或‘陷阱’能把我们吸到黑洞里去”。他的结论是要搞自己的芯片，自己的操作系统，自己的网管软件。中国现代国际关系研究所信息与社会发展研究室

主任俞晓秋也呼吁搞自己的东西：中国不仅有其他国家普遍存在的网络信息安全问题，还严重缺乏网络技术的自主性，“在核心技术上一直依赖国外企业，这才是最危险的”。

但也有不同的意见。来自信息安全国家重点实验室的荆继武教授说，关于“三大黑洞”我想反问一句：假设让我们国家自己开发一套操作系统，你认为我们的 BUG 会比微软的多还是少？“我认为会更多”。当然了，我们不用担心自己开发的操作系统里被人设后门做手脚，但如果里头 BUG 很多，其后果与“后门”或“陷阱”又有多大差别？一个 BUG 就是一枚炸弹。这就好比一只木桶，“这边烂那边烂都是烂”，你这个桶里只要有一块烂板子，其它的板子再长也没有用。如果是这样，你即使全部自己做“依旧会留下无限漏洞”，这是基本的工程原则。自己开发还有个能否产业化的问题，技术上过了但产业上不去还是受制于人，从经济视角看也无法承受。当然，荆并不否认“做自己的东西也是必要的”，如果你有这个能力的话。但这需要实力和时间。

出路何在呢？长远看包括“中国芯”在内的核心技术肯定不能放弃。我们是个大国，在事关国家安全和国民经济命脉的核心技术上长期受制于人，显然不

是明智的选择。但另一方面，全面拥有自己的核心技术也是不现实的，在可以预见的时间里能部分接近或达到世界水平，开发出几样“刹手锏”来已是难能可贵了。这就又涉及到“不安全文化”和“与危险同行”的话题了。但事情也许如同荆继武所说，“并不是不开发自己的东西就一定完蛋”，应对的办法是体制和管理。荆认为没有可以 100％相信的人，也没有 100％的安全可言，假如微软能留后门，你雇来开发系统的人就不能？即使自己的亲戚也未必靠得住，出路只能是用体制和管理来解决。“不能说国外的就不能用了，但需要用一个与他能力一样强的人监督他。”由此得出的结论之一将是：对于信息安全来说，“中国芯”也不是万能的，尽管我们万万不能放弃。

黑客威胁：打击伊拉克就意味着电脑病毒大规模爆发

一名同情恐怖分子以及伊拉克的马来西亚籍病毒作者警告称，如果美国对伊拉克进行军事打击，他就会在网上传播病毒。

据悉，这个自称为 MeLhackeR 的病毒作者的真实姓名可能

是 VLadImorChamLkovIc，被认为编写或参与编写了 VBS.OsamaLaden@mm、MeLhack、KamIL、BLeBLa.J

和 NedaL 五种蠕虫病毒。

MeLhackeR 证实了此前报道所称的他已经开发和测试了一种代号为 Scezda 的“三合一”超级病毒，该病毒集 SIRCam、KLez 和 NImda 的特性于一体。他说，这是一种真正的互联网蠕虫病毒。如果美国发动对伊拉克的军事打击，我就会传播这一病毒。他表示，自8月份以来，他一直在实验室对这一病毒进行测试。另外，他还证实了有关他与俄罗斯和巴基斯坦黑客有联系的报道。

IDefense 公司的总裁兼 CEO 布赖恩表示，尽管 MeLhackeR 没有能够证明他具有“培育”新蠕虫病毒的能力，但这种病毒很难被阻止。上周，IDefense 公司悄悄地警告其客户可能会有这样的病毒在互联网上传播，并表示，如果伊拉克受到攻击，企业应当提高警惕，严密监视可疑的互联网数据流量和电子邮件。布赖恩说，如果 MeLhackeR 获得成功，后果将是十分严重的。

McAfee 公司的副总裁文森特表示，Scezda 造成的威胁程度完全取决于MeLhackeR是否能够成功地把它传播出去。文森特说，如果他能够成功，造成的威胁是十分巨大的。由于由许多病毒最后都没有掀起多大风浪，因此造成的威胁很难预计。

据 IDefense 上周发布的一份公告称，亲伊斯兰和亲恐怖组织的人员开发的恶意代码的不断增加，尤其是在马来西亚，已经成为一个大问题，需要密切关注。布赖恩说，也许伊斯兰或恐怖组织的成员不足以引发严重的电脑问题，但这些组织的同情者却可能成为它们发动电脑战的代理人。

打击恐怖主义？欧盟关于网络监视之争加剧

美国东部时间 11 月 24 日(北京时间 11 月 25 日)消息，目前，欧盟正在进一步采取措施，以图制定出对通过电信公司及 ISP 进行信息收集活动加以限制的公共活动准则。欧盟的这些行动重新点燃了人们这样做会不会侵害公民自由的新一轮争论战火，某些工业界及政界官员不仅质问道：这些努力究竟对打击恐怖主义有何益处？

欧洲议会的一名议员认为，制定互联网监视公共准则的努力纯属浪费时间和精力。

欧洲议会议员、意大利人马科卡帕托对欧盟 15 个成员国中支持对所有欧盟公民电子邮件和电话进行“地毯式”监视的国家政府提出严厉批评，他解释说，之所以批评他们的这种做法，不仅因为这些方法侵害公民自由，还因为这些努力并无助于打击恐怖主义。他指出，在打击恐怖主义方面，提高获取恐怖情

报的能力比收集大量关于平民的数据信息要重要得多，因为“这样远不能把更多安全带给公民，而且，欧盟在这方面的做法已经起到了转移更为有效的情报收集活动资源与精力的负作用”。

当前，大多数欧盟国家赞同建立一条关于网络数据保留的公共原则，其中许多国家已经着手起草这方面的政府法律。

欧盟轮值主席国丹麦则不太赞同这一做法，但它准备提议各欧盟国家自己制定一些内容接近的网络数据保留法律，而不愿意强制性地要求每个成员国都必须遵守同一部单一法律。

据部分面临若延长数据保留期限成本就将增加的服务商称，丹麦欧盟轮值主席这样做实际上是朝着解决问题的正确方向迈出了实质性的一步。欧盟负责欧元 ISPA 贸易组织的事务经理乔迈克内米认为，丹麦官员正打算听取某些服务商的意见，“这一做法比以前可取多了，也透明多了”。

丹麦欧盟轮值主席没有立即对此事作任何评论。

吴基传部长在首届互联网协会会员大会上的致辞

各位来宾、各位代表，同志们：

首先，让我代表信息产业部，对大会的召开表示

热烈的祝贺，向与会的各界朋友表示诚挚的欢迎。

中国互联网协会第一次会员大会的召开，标志着中国互联网的事业的发展进入了新阶段，表明互联网会员单位从此有了自己的群众团体组织。互联网从她进入商用以来，就以强劲的生命力，推动着社会生产力和人类文明的发展，为世界各国人民提供了更加简便的工作和生活方式，使我们进入了一个资源共享、信息共享的新时代。其发展之快、影响之广是前所未有的。当然，与其他事物一样，互联网在其告诉发展中也带来了一些困难和问题。近几年出现的网络泡沫就是发展中的问题，反映出人们对互联网的认识有个由浅入深、由表及里的过程。通过深刻反思和认真总结，我们就能进一步把握互联网发展的本质和规律，不断克服前进中的困难，使互联网焕发出更大的生机与活力，为人们提供更好的服务。

我国的互联网坚持从国情出发，坚持稳健务实的政策，保持了良好的发展势头，用户数量、网络规模、技术水平、业务种类等方面都由较大的进展。据中国互联网络信息中心统计，截止 2002 年 9 月底，我国互联网用户数已达 5435 万，上网计算机已达 2056 万台，www 网站已达 81907 个。电子商务、远程教育、远程医疗、电子娱乐、电子政务等新业务系统层出不

穷，电信、银行、证券、能源、交通、教育等行业信息化应用程度也不断提高，互联网征逐步深入国民经济各领域和广大人民群众生活的各个方面。据估计，2001 年我国互联网市场规模已达到 70 亿元人民币。

但我们也清醒地看到，我国互联网发展的层次还比较低，与发达国家相比有着较大的差距。尤其是当前还存在着一些问题，如：网上中文信息资源较少，对我国传统文化形成了冲击；网络与信息安全体系不健全，利用网络从事违反法律、道德的网络犯罪问题日益突出；信息资源开发程度较低，互联网应用水平有待提高等。这些问题都需要我们认真加以研究和解决，否则将影响或延误我们的发展速度，影响我国互联网综合实力的提高。

当前，我国互联网发展正迎来一个非常好的机遇期。刚刚闭幕的党的十六大进一步提出了：“以信息化带动工业化，以工业化促进信息化”的发展战略，并强调要：“优先发展信息产业，在经济和社会领域广泛应用信息技术”，要把互联网站办成传播先进文化的重要阵地。这些重大决策的提出，必将加快国民经济和社会信息化进程，给我国互联网的发展带来了难得的机遇。另外，随着我国经济的快速发展和有关法律、法规的制订，互联网产业的大环境也在逐步好

转。我相信，我国互联网界一定能抓住当前的历史机遇，与时俱进，开拓创新，把我国互联网发展到一个新水平，使其在促进生产力发展、推动社会文明进步和提高人民生活质量等方面发挥更大的作用。

下面，对我国互联网的发展提出几点建议，供大家参考：

一、遵循客观经济规律、保证互联网健康发展。互联网可以改善和提高物质经济增长的方式和效率，但不可能取代物质经济的发展。那种认为“网络经济可以代替一切、改变一切”的观点是违背客观规律的，因此，我们必须注重应用而不能热衷于炒作概念，必须建立有效的盈利模式而不能着眼于“圈钱”，必须建立完善的产业链、充分发挥各方面的资源优势，理性务实地推动互联网的发展。

二、大力开发中文信息资源，推动网络文化多元化。要组织协调各方面的力量，大力开发中文软件和信息源、数据库，加快建设各类“数字图书馆”、“数字博物馆”，将历史上有代表性的典籍、文献进行数字化处理，通过网络传播我国优秀传统文化、现代科学技术和国外的先进文化成果，积极推进网络文化多元化，真正把我们的互联网站办成传播先进文化的重要阵地。

三、增强安全防范意识，健全网络与信息安全体系。应在加大宣传力度、提高全社会信息安全意识的同时，加强信息安全立法和技术标准的制定，建设多路由的物理网络，提高网络在各种情况下的自愈容灾和抗打击能力，并加快开发防止病毒、黑客攻击的信息安全技术，努力构筑一个技术先进、管理高效、安全可靠、建立在自主研究开发基础上的国家信息安全体系。

四、积极培育市场，提高互联网应用水平。要切实面向用户，找准业务增长点，加快开发用户乐于消费、能够消费的业务，积极探索和建立有效的服务模式和经营模式。要拓展用户层面，大力开发能够满足人们各方面需要的信息源和数据库，扩大全社会的信息消费，培育和发展互联网应用市场。当前要抓住实施以信息化带动工业化战略的机遇，加快将信息网络技术推广应用到社会经济生活的各个领域，切实提高我国互联网的应用水平。

五、努力营造一个良好的、有利于持续发展的外部环境，形成健康向上的氛围，同时增强互联网会员单位的自律，共同遵守社会道德秩序和规范，把我国互联网办成一个既有先进技术又有优质服务、既有先进中华文化特色又有开拓创新精神的繁荣、丰富、健

康的互联网体系。

首届中国互联网大会今天开幕主题是应用创新

今天（25 日），由信息产业部批准、中国互联网协会主办的“第一届中国互联网大会暨展示会”，在上海国际会议中心隆重召开。据会议的主办者介绍，这两年中国互联网增长速度减缓，因此，探讨中国互联网如何在应用上创新，为互联网在中国的进一步发展指明方向，成为本次大会的主要目的。本届大会的主题就是“互联网的应用——呼唤创新”。

本届大会是中国举办的行业层次最高、规模最大的互联网盛会。

中国互联网协会理事长胡启恒对记者表示，“整个中国互联网行业的当务之急是要把握机遇、迎接挑战，找准中国互联网的增长点。”

由于这两年中国互联网增长速度减缓，因此探讨其如何保持健康发展、如何在应用上创新，并为互联网在中国的进一步发展指明方向，将是这次大会的主要目的。

据悉，大会将全方位探讨的议题有电子政务、电子商务、网络经营、东西部地区互联网建设、下一代互联网和 IPV6、宽带网建设和骨干网技术、无线和移

动互联网技术、中国电子口岸简介、网络与运行技术、网络与信息安全、行业政策和法律建设、网络文化建设与网络信息资源开发、互联网知识产权保护等。这些涉及到互联网应用、技术、管理、知识产权、网络安全和互联网健康发展的全新议题，将呈现出层次高、视角新、范围广、应用强的显著特点。参与演讲的互联网专家、学者、企业界人士共有 100 位左右。

美研究人员正在研究阻止电池黑客的对策

一个由计算机科学家组成的小组正在对一种新型的拒绝服务攻击进行研究。这种攻击的对象主要是以电池为能源的设备。美国弗吉尼亚州技术学院电气与计算机系的TomMaRtIn教授获得了美国国家科学基金会批准的 40 多万美元的科研费，用来研究一种方法，防止以电池为能源的计算机在这种安全攻击中把能源耗光。

虽然研究人员承认这种攻击很少出现，但是，笔记本电脑、掌上电脑、tabLetPC、网络手机和其它设备的普及使这种设备成了诱人的攻击目标。

对于使用电池备份系统防止由于停电给数据库和存储系统造成损失的企业来说，这种威胁就更可怕。

MaRtIn 教授说，如果一个系统在停电期间使用电

池备份装置，针对电源的攻击能使电池备份装置在电源恢复之前失效。我还不知道这种攻击的实例，但是，这项研究就是要防止这种攻击流行，通过展示潜在的攻击效果和解决方案来缓解这种攻击。

MaRtIn 教授和他的同事们研究了可能对以电池为能源的计算机实施攻击的三种手段和应对措施。

第一种是服务申请攻击，黑客在网上反复发出服务请求。在这种情况下，受害人无论是否理睬这种请求，其电池能源都将消耗得很快。第二种攻击可能包括能源病毒，受害人将被迫反复执行一种非法的、耗能量非常大的程序。第三种是黑客使用恶意的电源病毒，在这种病毒中，程序经过修改将消耗更多的能源。

这个研究小组正在探索一些方法为移动计算设备制作一个识别架构以保证最低的电池寿命。研究的另一个重点是设计一种识别与能源有关的安全漏洞的方法。

MaRtIn 教授说，我指望看到的最终结果是为移动计算机设计人员提供一套工具来查找他们系统中与电源有关的安全漏洞，为他们的修复这些漏洞提供一个指南。不过，现在最好是首先不要公开这些安全漏洞。

银行金融业易遭受数据库漏洞危害

1 月 23 日，据发布的一份民意调查显示，银行和金融业的数据库软件开发人员报告的安全性漏洞比其他任何行业的数据库开发人员报告的都多。

EvansDataCorp.市场调查公司对700名为美国企业和软件开发公司工作的数据库开发人员进行的调查显示，其中 12%的被调查者表示，他们支持的数据库在去年遭受过安全性漏洞方面的问题。

这份在去年 12 月进行的调查用三个一般性定义说明了安全性漏洞的特征：可以成功摧毁或删除数据库数据的计算机病毒、人为操作失误对数据库产生的破坏或未经授权而非法进入数据库。在这些产生漏洞的方法中，计算机病毒被认为是导致错误的最常见途径。

银行和金融服务业中大约 27%的被调查的开发人员都提到，他们在去年遭受过安全性漏洞破坏。在医疗和卫生保健行业，18%的数据库开发人员都遇到过这类漏洞的破坏。在电信行业，相同比例的开发人员也遇到过这类漏洞的破坏。同时，有 12%为电子商务和其它因特网公司工作的开发人员报告了安全性混乱问题。政府和军事机关中，9%的开发人员也都遇到这类漏洞。

参加该调查的数据库开发人员所使用的数据库软件来自各个不同的供应商。最常用的应用软件包括微软公司的 SQLServer、IBM 公司的 DB2 和 Sybase 公司及 ORacLe 公司的数据库软件。大约 70%的参加该调查的开发人员都提到，他们所支持的数据库来自以上这些供应商中的两家或更多家。

除了带有防火墙和网络身份验证的安全性保护外，数据库一般包括内置的安全功能，如数据加密等功能。但是，仅有 37%的被调查者提到他们使用过内置的安全功能。

同时，据报道有些数据库安全缺陷（包括微软 SQLServer 中的一个漏洞）在用户注销数据库的短暂过程中易被黑客攻击。在去年 12 月发现的微软数据库软件中的另一个漏洞会使该软件遭受“拒绝服务”攻击。PGP 安全公司的 CoveRtLabs 部门也于本年 6 月在 ORacLe 的 ORacLe8I 数据库中发现了易被黑客攻击的安全漏洞。

在该市场调查公司进行调查的这 700 名开发人员中，其中的四分之一人员所在的公司有超过 1000 名员工。70%的数据库开发人员在企业内部工作，而另外 30%的人员在软件开发公司工作。

高端网关:融专用 IC、防病毒、防火墙于一体

日本图研 NetWave 于 2002 年 11 月 22 日发表了具有防病毒和内容过滤等主要安全防卫功能的高端网关“FortIGate3000”。通过采用 ASIC（特定用途 IC）提高了处理性能，该公司强调：“与现有的网关型防病毒软件相比，处理速度可以提高数十倍以上”（产品开发商美国 FortInet 总裁兼首席执行官 KenXIe）。价格为 523 万日元（约合人民币 32.7 万元）。2003 年 1 月上市。

目前除图研 NetWave 外，日本 CTCSP、日本 DataContRoL 以及日本 ForvaLcReatIve 公司也在销售 FortInet 的产品，估计各公司将于 2002 年年底至 2003 年初上市 FortIGate3000。

FortIGate 系列产品利用一套硬件来处理“防病毒”、“防火墙”、“VPN（虚拟专用网络）”以及“内容过滤”等主要安全功能。通过采用 ASIC 和专用 OS，提高了处理性能。在日本国内，除日本赛门铁克以外尽管主要防病毒开发商都已经率先上市网关型防病毒软件，但图研 NetWave 董事长兼总裁高谷英一表示：“我们将凭借防病毒处理性能和综合安全功能拉开与网关型防病毒软件的距离”。

作为防病毒功能，除HTTP和SMTP外，还支持POP3和 IMAP 等协议。还建立了发现新型和变形病毒或得到通知以后，4 个小时内就能够进行更新并发布的防病毒体制。

该产品具有 3 个千兆位以太网接口。利用 3DES 加密时 VPN 的处理速度为 300MBit/秒。VPN 的通道数为 5000。还具有利用关键词和 URL 等过滤内容的功能。

FortIGate 系列产品除高端款式的 FortIGate3000 外，目前还在提供 7 款以 20 个用户的小型运营商为对象的“FortIGate50”（16 万 6000 日元，约合人民币 1 万元）等产品。

美专家呼吁建立新的灾难报警系统

美国一个由政府部门、研究机构和私营企业部门应急反应专家组成的委员会 11 月 25 日发表一篇报告称，美国各地的应急警报系统需要重新改造，并将采用一种强制性的信息标准。这个委员会认为，目前杂乱无章的警报系统，包括应急警报系统和国家海洋大气局气象广播等，工作状态都不好。

这篇报告指出，由于许多联邦机构负责报警，没有一个单独的联邦机构肩负明确的责任来管理全国的、全面灾难性的、公共报警系统的开发和有效地应

用。新组建的国土安全部应该担负起这个责任。

美国总统布什 11 月 25 日签署了 2002 年国土安全法案。这个法案把移民归化局、移民归化局、海岸警卫队和保密局等置于一个内阁级的部的管辖之下。这篇报告称，新的机构现在应该制定把紧急信息传递给美国公民的方法。

新的报警系统必须能够与各种设备通信，包括计算机、手机、传呼机和其它新的电子设备。因此，这篇报告指出，XML 最有可能成为这种报警系统采用的协议，其它协议可用于非计算机平台。

报警信息必须具有独特的识别码，具体说明地理区域的不同的警报等级，并且具体说明加密方式以证实发送信息者的合法身份。这个委员会还呼吁对这种报警系统的有效性实施进一步的研究。

2002 年国土安全法案规定，国土安全部负责提供恐怖主义分子活动的警报。

.Info 域名系统遭到大规模攻击

互联网域名管理公司 ULtRaDNS 首席执行官 BenPetRo 介绍说，上个星期四（11 月 21 日）上午，该公司的网络服务器遭到了四个小时的拒绝服务攻击。这次袭击每秒种向每个连接互联网的服务器发送了将近 200 万个服务申请，潮水般的数据向该公司的

服务器涌来，使该公司的网络管理人员费了很大的气力才保证托管.Info 和其它域名的服务器继续运行。

PetRo 说，这是我所见到的规模最大的一次袭击。他强调指出，这次袭击对该公司的核心域名系统服务没有造成影响。不过，网络管理人员必须迅速处理情况，封锁攻击。从网络管理的角度说，这次攻击使我们提高了警觉。

这次袭击与一个月前发生的针对DNS根服务器的袭击几乎完全相同。PetRo 说，调查很可能正在进行当中。不过，联邦调查局和 ULtRaDNS 公司的自己的服务提供商 WorldCom 公司的 UUNet 没有立即对此事发表评论。

不过，调查人员会发现，这种事件的调查是非常困难的。这种攻击一般称作分布式拒绝服务攻击。在攻击开始前，黑客首先控制一些服务器，然后从这些服务器发起攻击。由于经过了两次重新定向，很难发现黑客的踪迹。

但是，PetRo 表示，找到这些黑客的重要性越来越大了。因为，最近的攻击趋势已经从攻击企业网络转向了攻击互联网本身的基础设施。他说，如果你攻击 Amazon.com，你伤害的只是亚马逊公司。如果你破坏.com、.org 和.net 等域名服务器，你就是在伤害

整个国家。

ULtRaDNS 是互联网协会的成员，从明年开始成为.org 域名的主要提供商，目前负责管理.Info 域名和爱尔兰、卢森堡、挪威和其它 9 个域名。

美国在线阻截了利用 Windows 功能的垃圾消息

互联网服务厂商美国在线公司于当地时间 11 月 25 日宣布，它已经对其网络进行了适当的变化，使第三方厂商不能向其订户发送弹出式垃圾信息。

上周，垃圾信息发送者于上周发现，美国在线公司对其网络进行了一些技术性的改变，阻止第三方厂商向订户发送一种较新类型的垃圾信息，该信息利用了 Windows 的消息服务。

美国在线公司的发言人安德鲁威恩斯坦表示，在与垃圾邮件的战争中，对于我们的订户而言，这是一个巨大的胜利。

这一技术使用了Windows中的一项让网络管理人员向客户通知服务器当机或计划性的备份等重要维护问题的功能，尽管弹出的对话框只能显示文本字符，但它能够出现在所有窗口的上面，而且要求用户必须作出反应。Windows95、98、NT、2000 和 XP 都存在着这一问题。

DIRectAdveRtIseR 和 BRoadcastMaRketeR 等公司的软件允许直销商每小时向随机的互联网地址发送数以十万计的消息。每成功发送一次消息，就意味着一个台式机的桌面上就会弹出一条消息。垃圾邮件发送者非常喜欢这种技术，因为它能够强迫互联网用户看到消息，并关闭窗口。

BRoadcastMaRketeR 公司的总裁 AnIshDhIngRa 表示，响应率非常高。DhIngRa 称，这一技术不是缺陷，因为受影响的用户可以简单地关闭该使弹出式菜单出现的 Windows 功能。他表示，他的公司的软件将在未来几周后“冲破”美国在线公司的封锁。

这可能意味着，美国在线公司会发现自己已经陷入了一场军备竞赛。美国在线公司的威恩斯坦说，我们已经成功了阻止了垃圾信息发送者对该技术的非法利用，我们将继续阻击垃圾消息。

美软件公司员工实施前所未有 ID 盗窃犯罪

美国纽约州联邦地方检察官和联邦调查局 25 日逮捕了三人组成的信用卡盗窃集团。该集团涉嫌盗窃 30000 人的信用卡账号，他们从被害者银行账户提取资金并且向第三方出售信用卡用户信息。信用卡盗窃集团的犯罪金额超过 270 万美元。美国联邦政府官员说，这是有史以来最大的 ID 盗窃案件，美国主要媒

体都对案件做了报道。

据检察官和 FBI 的调查，盗窃行为是由 33 岁的 PhILIpCummIngs 实施的，他是位于纽约州的软件企业 TeLedataCommunIcatIons 公司技术支持部门的主要负责人。TeLedataCommunIcatIons 公司的业务是向金融机构和一般商业企业提供专用的信用卡信息传输软件，该软件的功能是从将信用卡公司的信用信息传输给有关金融机构。

CummIngs 利用工作条件的便利，利用从客户企业拿到的密码和账户盗窃信用卡公司的信用卡用户报告书，然而在从信用卡用户的银行账户中提取资金，用于个人购物和其他消费。同时，CummIngs 还将盗窃的 ID 信息卖给了其他的信用卡盗窃集团。

信用卡用户报告书包括了用户的所有详细资料，目前调查当局正在全力调查因被害的详细情况。

IDC 称西欧将增长用于计算机安全的支出

IDC 公司在对 2002 年欧洲公司基础设施的消费情况进行调查后称，尽管资金紧张，IT 支出中用于安全解决方案的比例将增加。

调查结果显示，由于运营环境连通性的提高，并面临复杂的威胁，安全已成为对欧洲首席信息官们的头号挑战。

IDC 安全产品和战略服务部门的 ThomasRaschke 说：“在一个协作商业和供应链集成的年代里，安全已不仅是为了保护机构免遭威胁的必要支出，而且成为了一个真正的商机。”

但据 IDC 称，如今企业对安全的投资仍是因为担心存在安全漏洞。

据 IDC 称，欧洲公司目前使用的三大安全技术是反病毒、防火墙软件和基于硬件的防火墙应用软件。

公共密钥基础设施（PKI）和单次登录（SSO）是欧洲最热门的安全技术。分别有 17%和 14%的欧洲公司计划在未来 12 至 36 个月内启用这些技术。

美政府和企业共同推出安全人员资格认证计划

负责考试的产业与政府联合机构的代表说，一项新的针对入门级计算机安全专业人员的认证项目将在周一正式启动和运作。

计算机技术产业协会提出的计划名为 Security+认证，它可能成为帮助公司和政府机构雇佣懂行网络管理人员的一项最低要求。计算机技术产业协会由二十几位行业和政府安全专家组成，其中包括来自微软公司、IBM 公司和联邦调查局的代表。

计算机技术产业协会 Security 项目管理人说，

这个项目将成为安全专业人员的入门标准，它是对专业知识的确认。

根据帮助制定标准的各个专业机构的判断，Security+认证看起来是成为检验标准的一个步骤，新的标准标准将测定一名未来的安全人员是否能够充分理解安全概念。计算机技术产业协会的成员还有 Sun 微系统公司、VeRISIgn 公司、国家保密局和国家标准与技术研究院，后者的职能是确定非军事政府机构的雇佣标准。

自去年 9 月以来，布什行政当局公布了保障网络安全的国家安全战略草案，此后安全认证获得了突飞猛进的发展。该战略强调，需要更多的安全培训和更好地做好安全技能认证工作。

国家安全战略指出：安全专业人员、机构和其他适当组织应当研究国家组织的安全认证计划的可行性。包括继续教育和重新考试计划。联邦政府应当帮助建立这些计划。如果计划已经建立，应考虑适当地对联邦 IT 安全人员进行认证。

我国台湾培养黑客来防黑每日学费过万

要防范黑客攻击，就得先学习黑客的本领，做到知此知彼。

美国信息安全公司 Foundstone 日前在我国台湾

举办了“骇客实战研习营”，台湾省和香港特区有关机构、企业共派了 26 人（有两个女学员）接受培训，这些学员们将学习和模拟黑客的攻击技巧及防御技术，他们要签下不得从事黑客行为的协议。培训他们的机构将为他们交上学费，为时 4 天共计 18 万元（“新台币”，约合 4 万多元人民币）。

Foundstone 这次活动是与台湾省精诚资讯公司合作推出的，一位名叫陈彦铭的讲师曾协助微软检查“.net”系统。他在新闻招待会现场演示了黑客如何利用浏览网页源代码、来寻找价格、进行编辑等步骤，把使用特定程序建构的购物网站，把定价 2755 美元的商品窜改成只售 1 美元。

学习黑客入侵技巧是为让信息技术人员能够知己知彼、百战百胜，也可了解自己公司系统是否有漏洞，从而进行改善、建构更安全的网络环境，这种人被称为“白帽”黑客，“黑帽”黑客则较偏向“黑暗面”。

这一课程为每年一度美国拉斯维加斯举办的“黑客大会”指定技术训练课程，在海外的美、英、日等地巡回开讲，曾参加培训的机构包括 AT&amp；T、波音、微软、雅虎与美国太空总署、国家安全局、陆海空军等，我国台湾联电曾派人参加过这个培训。

据我国台湾媒体报道：这一课程上使用的教材、设备、讲师都是从美国“空运”来的，学员上课时使用装有Windows2000与Linux双操作系统的特制笔记本电脑，他们不仅要学习上百种黑客入侵技巧，毕业前还必须以所学技巧来尝试入侵网上的一个虚拟公司网站，并取得指定的文件。

首届互联网大会闭幕中日韩互联网协会结盟

在今天闭幕的首届“中国互联网大会”上，中日韩三国互联网协会为推动三国的互联网发展结成共同联盟，同期签署了谅解备忘录。

中国互联网协会(ISC)、日本互联网协会(IAJ)、韩国互联网协会(IAK)相关人士今天在此间表示，为实现中日韩地区互联网及相关事务的发展、推动宽带互联网络基础设施与业务应用结成联盟。

联盟活动的主要目的包括：支持中日韩三国政府在互联网行业发展方面所作的工作；积极推动亚太地区互联网技术与应用的普及，改善该地区互联网信息交换的质量与效率；继续召开亚太地区互联网宽带峰会(ABS)，该峰会将在中日韩三地轮流召开。

据悉，该联盟将与其它互联网组织合作，努力成为亚太地区互联网活动的核心。

另悉，为期三天的中国首届互联网协会今天在上

海闭幕。会议就中国互联网的发展政策及趋势、电子政务、电子商务、宽带技术与建设、网络与信息安全、互联网经营模式以及下一代互联网等议题进行了探讨。

英国 1/8 电子邮件是垃圾 邮件用户倍受折磨

据 MessageLabs 的调查结果显示：在英国 8 份电子邮件中就有 1 封是垃圾邮件。然而，在美国情况更糟，垃圾邮件几乎是英国的两倍。

根据邮件安全公司 MessageLabs 的最新数据显示：2002 年英国的电子邮件用户倍受垃圾邮件折磨。

据 MessageLabs 估计，在英国 1/8 的邮件是垃圾，而去年 1 月份垃圾邮件比例仅为 1/199。根据美国的现状分析，其情况更糟，约有 1/3 的邮件是未经要求的广告垃圾。

MessageLabs 首席技术官 MaRkSunneR 说："6 到 9 个月之前，垃圾邮件还不太严重、甚至觉察不到其存在。但是现在却铺天盖地。"

他还说，邮件过滤阻止技术现在越来越复杂，包括垃圾变种识别技术，一些垃圾邮件为了避免过滤而稍作了改动，垃圾邮件发送和反垃圾是魔高一尺，道高一丈。

MessageLabs 公司在欧洲、美国及英国提供电子

邮件管理服务，该公司称，在 2002 年每分钟阻止 45 条垃圾信息。

除了垃圾邮件处理费时费力外，垃圾邮件还会带来病毒及危害计算机安全。MessageLabs 公司称，所谓的 NIgeRIanscam,或 419scam 今年扩散尤其快。

邮件软件厂商不得不在其新产品中加入复杂的垃圾过滤机制，微软的 OutLook 和苹果公司的邮件程序都在最近增加了新的垃圾过滤功能。

MessageLabs 公司的数据是对几家邮件软件厂商过去几周的调查得出的，结果显示在几年底之前垃圾邮件呈上升态势。

MessageLabs 称，今年 9 月份在英国垃圾邮件最为猖狂，平均每 5 封邮件中就有一封是垃圾，最好的时间情况是 2 月份，垃圾邮件率降低到 1/251。

计算机网络安全

留级生病毒

警惕程度：　　发作时间：随机

病毒类型：蠕虫病毒　传播方式：邮件/局域网

感染对象：局域网

病毒介绍：

病毒运行后会终止没有内存监控功能的某些国内杀毒软件的运行，并将自己复制到系统目录下登记为自启动。将浏览器标题修改为："You must tell me why I only have 40 for the c exam!"，利用自身带的密码字典破译所有局域网计算机的密码，破译后该病毒会释放出一个可感染文件的病毒感染局域网中每一台计算机中的所有可执行文件，病毒破译密码和感染文件的过程中会使局域网瘫痪。企业级用户要特别注意防毒。

病毒的发现与清除：

此病毒会有如下特征，如果用户发现计算机中有这些特征，则很有可能中了此病毒：

1．病毒运行时会将自身复制到系统目录下，命名为：restudy.exe。

2．病毒会修改注册表，在 HKEY _LOCAL _MACHINE\ Software\ Microsoft\ Windows\Current Version \Run 启动项中添加键值 restudy,该键值的内容是病毒的文件路径，这样在下一次启动计算机时，病毒会自动运行。

3．病毒会遍历局域网，并尝试把自己复制到其它计算机的如下位置：\\admin$\\restudy.exe。

4．将 IE 的标题改为："You must tell me why I

only have 40 for the cexam!”。

5．病毒执行后首先终止下列反病毒主程序：kfw.exe、kfwmain.exe、vptray.exe、PFW.exe、PFWmain.exe、kav32.EXE、KAVSvcUI.EXE。

用户如果在自己的计算机中发现以上全部或部分现象，则很有可能中了“留级生”（Worm.Restudy.21）病毒。

QQ 连发器病毒

警惕程度：　　发作时间：随机

病毒类型：木马病毒　　传播方式：QQ 软件

感染对象：QQ 用户

依赖系统：WIN9X//NT/2000/XP

病毒介绍：

该病毒运行后会偷偷藏在用户的系统中，并修改注册表进行自启动。发作时会寻找 QQ 窗口，每隔 1 分钟就给被感染用户的所有线上的 QQ 好友发送诸如“快去这看看，里面有蛮好好东西 ”之类的假消息，诱惑用户点击一个网站，如果有人信以为真点击该链接的话，就会被病毒无情感染，然后成为毒源，继续传播。

病毒的发现与清除：

此病毒会有如下特征，如果用户发现计算机中有

这些特征，则很有可能中了此病毒：

1．病毒运行时会将自身复制到系统目录下，命名为：WebAuto.exe。

2．病毒会修改注册表，在 HKEY _LOCAL _MACHINE \SoftwareMicrosoft\Windows\Current Version\Run 启动项中添加键值 WebAuto.exe，该键值的内容是病毒的文件路径，在下一次启动计算机时，病毒就会自动运行。

3．病毒会将用户系统中的 IE 默认首页改为：http://www.qq588.com ，使用户一上网就中招。

4．病毒会寻找 QQ 的发送消息窗口，给用户所有好友随机发送以下消息：

1．“激情电影爽啊！给你也推荐一下，完全免费”；

2．“快去这看看，里面有蛮好好东西”；

3．“上次看了个网站不错，去看看吧”；

在这些消息之后还伴随着一个恶意网址诱骗用户点击。

用户如果在自己的计算机中发现以上全部或部分现象，则很有可能中了 QQ 连发器。

Bat.muma 病毒

病毒名称：Bat.muma　　病毒类型：蠕虫

危害级别：中　　传播速度：高

技术特征：

该病毒采用批处理命令编写，并携带端口扫描工具，通过暴力破解被攻击的计算机超级用户密码，进行疯狂传播。

病毒行为：

1、病毒可能复制以下文件到系统目录

10.bat	hack.bat
hfind.exe	ipc.bat
muma.batv	near.bat
ntservice.bat	ntservice.exe
NTService.ini	nwiz.exe
nwiz.in_	nwiz.ini
ipcpass.txt	tihuan.txt
rep.exe	psexec.exe
random.bat	replace.bat
ss.bat	start.bat

pcmsg.dll

2、病毒由 Start.bat 开始运行。这个批处理程序会调用其它批处理程序去完成传染；

3、病毒会搜索从 C：到 H：盘中\MU 目录以及其了目录下的所有文件，并把文件名保存在 LAN.LOG 文

件中。当被搜索的文件名中包含“MU”字符串时，nwiz.exe 将被执行，nwiz.exe 根据 nwiz.ini 和 nwiz.in_文件对病毒中的字符串进行简单的加密。这个搜索过程完成后，LAN.LOG 会被删除；

4、删除 ipcfind.txt 文件，调 HFind.exe 进行网络扫描，搜索网络中的计算机。并试图使用以下的密码去破解被攻击的计算机。可能的密码是：

password	passwd
admin	pass
123	1234
12345	123456

<密码为空>

5、被 HFind.exe 破解成功的计算机，会被病毒将上述的所有文件通过管理员文件共享方式拷贝到其系统目录下。对于 Windows NT、Windows200 系统是 C:\winnt\system32 目录,对于 WindowsXP 系统是 C:\winnt\system32 或 C:\Windows\system32 目录，对于 Win9X 是 C:\windows\system 目录；

6、传染成功后，病毒会用 Psexec.exe 程序远程启动被感染计算机上的 Start.bat，从而使病毒在被感染的计算机上激活；

7、调用系统程序 netstat.exe，然后运行

Near.bat 从 netstat 的输出信息中获得更多的 IP，并对这些 IP 进行攻击；

8、ss.bat 创建或者修改系统中的 admin 用户，并设置其它密码为：KKKKKKK。为被攻击计算机留下一个后门。

9、利用 ntservice.bat 调用 ntservice.exe 为自己注册一个名为“Application”的系统服务，保证自己能在每次系统重启时被激。

MUMA(Bat.Worm.Muma)病毒

警惕程度：　　发作时间：随机

病毒类型：批处理病毒　传播方式：网络

感染对象：网络　依赖系统：WIN9X//NT/2000/XP

病毒介绍：

该病毒是一个以“批处理文件”形式存在的蠕虫病毒，它构思巧妙，主病毒体采用批处理命令编写，不但自身携带一些病毒程序，还利用系统提供的正常程序阻塞网络。该病毒共由 9 个批处理病毒体组成，调用 7 个程序完成病毒的破坏工作，会扫描整个网段、端口，记录密码为空的计算机，并对这些计算机进行攻击。该病毒运行时还会将自身改装成一个服务程序，随系统启动，建立有管理员权限的新用户，并利用该用户登陆计算机，进行新一轮的网络攻击。

病毒的发现与清除：

此病毒会有如下特征，如果用户发现计算机中有这些特征，则很有可能中了此病毒：

1、该病毒由 start.bat、muma.bat、10.bat、replace.bat、ipc.bat、hack.bat、random.bat、ntservice.bat、ss.bat 等 9 个病毒体组成，并且调用 HFind.exe 、 ntservice.exe 、 nwiz_.exe 、psexec.exe、psexesvc.exe、rep.exe 等程序进行破坏，病毒运行时会将这些文件拷贝到系统目录下。

2、病毒运行时会使用 net use 指令，对密码为空或有简单密码的计算机进行 IPC 连接，远程启动 ntservice.bat 病毒文件，目的是在系统中启动一个名称为“Application”的“服务”，该服务会运行另一个病毒体“ss.bat”，用系统管理工具查看系统是否存在一个名为：“Application”的服务。

3、病毒还会利用“net user”命令在被感染的计算机中增加一个有管理员权限的新用户：admin，密码为 KKKKKKK，并以此帐号、密码登陆被感染机器（127.0.0.1），以管理员的身份调用 START.BAT，查看系统中是否存在这样的一个用户。

用户如果在自己的计算机中发现以上全部或部分现象，则很有可能中了 MUMA(Bat.Worm.Muma)病毒。

尼姆达最新变种病毒

警惕程度：　　发作时间：随机

病毒类型：蠕虫病毒　传播方式：局域网/文件

感染对象：系统文件

依赖系统：WIN9X//NT/2000/XP

病毒介绍：

尼姆达变种Ⅰ（Worm.Nimda.i）病毒在原尼姆达病毒编写的基础上又进行了技术改进，具有更强的泄密性与网络传播的能力。

虽然该病毒还未在全球泛滥，但鉴于该病毒的特性，瑞星反病毒工程师提醒个人及企业级用户，对该变种病毒要提前预防，以防止再一次发生尼姆达病毒袭击全球的事件。

病毒特性：

一、将被感染文件藏于自己体内。

该病毒的感染沿袭了原尼姆达病毒的感染方式，病毒运行时会查询注册表 SOFTWARE \Microsoft \Windows \CurrentVersion\ App Paths 的值，感染该项里的所有注册文件。感染时会将目标文件放入病毒的资源段内，即病毒不是将自身代码插入被感染的文件体内，而是直接将被感染文件“吞”到自己的肚子里。然后病毒会将自已的文件名改成被感染文件的

文件名，进行李代桃僵。当不知情的用户想运行原来的文件时，病毒便会首先取得运行权，然后从自己体内将原来的文件释放出来并执行，使用户无法查觉到异常。

二、运行时藏身 IE 体内。

病毒会通过查询注册表信息得到 IE（Explorer）的进程号，然后将病毒体注入到 IE 的进程空间内。如果成功病毒将在 explorer 进程空间中执行病毒的主体，这样病毒运行时就能躲过一些对内存比较了解的用户的查看。

三、以高优先级进行循环传染。

病毒运行时会提升自己的线程优先级，并且每隔 30 秒就重复一次传染流程，将导致系统资源极大浪费。

四、快速的局域网传播。

病毒运行时会枚举局域网内的所有计算机，并对其共享目录进行搜索，当病毒发现有系统文件时就尝试感染该文件。如被搜索目录存在 doc 文件时，病毒便会将自己复制到该目录下，并将自身命名为：_setup.exe 和 riched20.dll。只要用户双击该 doc 文件，系统便会自动执行这两个病毒文件，造成病毒在被感染的计算机上被激活，导致病毒再一次重复感

染动作。

五、严重的泄密特性

病毒运行时还将激活当前系统的guest账号并将其加入到管理员组中，使其具有管理员的权限，然后病毒就能通过该通道进行非法操作。病毒还会将当前的 a 至 z 盘变成共享，使任何外界的黑客程序都可以无障碍地访问计算机中的信息，并且病毒还会感染这些共享磁盘中的所有系统文件，使其全部带毒。

6 月 26 日警惕 CIH 病毒变种

CIH 病毒变种（CIH_13）

危害程序：高危

别名：CIH V1.3

该病毒可感染 Windows 95 和 Windows 98 的 EXE 文件。被感染的文件一旦被执行，就会常驻内存，并在目标文件中寻找未被使用的空间，并把自身添加到其中。

此病毒具有严重的破坏性，一旦爆发会覆盖电脑硬盘上的数据，随机的删改系统硬盘上的数据，而且数据还不容易修复。爆发日期为 6 月 26 日，可以感硬盘中所有的可执行文件。而且还会通过破坏 Flash BIOS 的数据存储对系统进行永久性的破坏，该病毒对 Windows NT 系统不具备破坏作用。

死神（Azrael）病毒

危害程度：中等

病毒类型：宏病毒

这是由一个自动打开的宏组成的小型宏病毒。在每月的 23 日发作，可删除 c:\windows\system\. 下所有后缀为.dll 的文件，感染后会覆盖就近文件列表中的 4 个文件和 C 盘下所有后缀为.doc 的文件。

威士尔（Win32.VCell）

危害程度：中等

病毒类型：Win32

这是一个 win32 变形病毒，不会驻留内存，它会自动搜索当前路径和目录下的 PE 可执行文，然后把感染所有找到的文件。

6 月 30 日发作时会显示以下信息：

W32/Cell Virus

My evolution is complete

Cell is born anew into the Win OS

why? because youll laugh

why? because Cell is in them

under your nose i have made more akin to me!

七月历来都是病毒高发期，许多病毒中的厉害角色纷纷粉墨登场，象不死毒王求职信变种在 7 月 6 号

发作，它利用 IFRAME 漏洞在受害者的电脑上来执行自己，而不需要用户运行附件。超级格式化病毒会在 2 号发作，除能终止一些杀毒软件运行外，还能在电脑重启时格式化硬盘，其它的病毒大多是高危病毒，触发机制、破坏方式五花八门，各不相同，七月的电脑用户在做好电脑散热措施的同时，千万别忘记做好病毒防范措施，保护电脑中的数据安全。

JS/Gigger.a 病毒

危害程度：高

病毒类型：蠕虫

爆发时间：2003.07.01

病毒描述：

JS/Gigger.a 通过互联网聊天通道传播感染，病毒通过发送带有如下信息的邮件传播自身：

主题：Outlook Express 升级

主体：MSN 软件公司

附件：Mmsn_offline.htm

附件就是该病毒主体。该蠕虫病毒利用 MAP1，通过微软 Outlook 联系和 Windows 地址薄发送自身，并在根目录和系统目标下生成如下文件：

C:\B.HTM

C:\BLA.HTA

C:\WINDOWS\help\mmsn_offline.htm

C:\WINDOWS\SAMPLES\WSH\Charts.js

%盘符%\开始菜单\Programs\StartUp\msoe.hta (在网络驱动器上)

C:\AUTOEXEC.BAT 将执行格式化 C 盘的命令。

病毒发作时，所有 SCRIPT.INI 文件被 mIRC 脚本命令所覆盖，这样只要其他用户加入到被感染用户所在的频道，病毒就会被送出。所有以.ASP、.HTM 和.HTML 为后缀的文件都将被病毒代码所覆盖。如果日期是 1 号、5 号、10 号、15 号或 20 号，其他所有文件的内容也将被删除，数据变为 0 字节。

解决方法：

升级病毒库到最新版，开启病毒系列软件的实时监控。