# 信息安全动态

8

主编：四川大学信息安全研究所

吉林科学技术出版社

# 前　言

为全面、及时地反映国内计算机信息网络安全领域的发展动态，四川大学信息安全研究所选择了国内发行的中央和省市级的日报与经济类报刊以及 IT 业重要报刊(入选报纸的发行量至少 5 万份以上、杂志至少 2 万份以上)，将其中涉及计算机信息网络安全在技术、产品、市场、管理、案例等方面发展动态的报道加以精选并分类整合，逐月汇编为《信息安全动态》，自 2001 年 1 月起，由吉林科学技术出版社正式出版。

《信息安全动态》全年二十四辑，每月出书二辑。我们期望以此来快捷、全面地反映国内信息安全领域的发展动态和国内计算机信息网络安全市场的一些基本状况，能为应用、管理、决策人员提供有益的参考。

因无法与部分作者取得联系，故我们依照有关规定将其稿酬代为保管，同时敬请这部分作者见到本书后及时与我们联系，届时我们会将稿酬及利息汇出。

限于编者的经验，不足之处敬请批评指正。

四川大学信息安全研究所

《信息安全动态》编委会

信息安全动态

# 目 录 索 引

## ✧ 一、*警钟篇*

## ✧ 二、管理篇



## ✧ 三、业界动态篇

## ✧ 四、技术篇

## ✧ 五、应用篇



## ✧ 六、综合分析与对策研究

## ✧ 七、趋势篇



## ✧ 八、曝光篇



## ✧ 九、安全锦囊

# 警钟篇

- 网络时代，勿忘安全
- 时代重大课题——信息安全保密
- 网络恶意攻击无时不在，网络安全意识令人堪忧
- 专家警告：今年病毒走网络、爱邮件、传播快
- 专家预测：全球病毒邮件可能巨增
- 最新病毒警告（9则）

……

金融电子化

2001年4月1日

# 网络时代 勿忘安全

中国科学院高能物理研究所 许榕生

许榕生，男，1947年1月出生，现任中国科学院高能物理研究所计算中心研究员、博士生导师兼中科院信息办专家组成员，从事互联网网络工程及网络安全软件课题。1970年北京大学数学力学系毕业，1981年获中科院研究生院硕士学位（粒子物理与计算机模拟），1987年获美国加州大学（Santa Cruz）博士学位（高能物理实验，软件与网络）。先后在美国的斯坦福、橡树岭国立实验室任博士后及访问学者，在西欧核研究中心研修WWW等网络技术。目前，负责国家重点基础研究发展规划项目及中国科学院"黑客入侵防范体系"等网络安全课题的研究工作。

我们的世界正在演变为一个电子化的世界（E－World），所有的信息正在全面数字化，电子世界中四通八达的网络把人们联系在一起。天涯变为咫尺，地理上的距离几乎都消弭于无形，人们真正作到了运筹帷幄，决胜千里。

这一切都应归功于电脑网络，而网络也已成为推动各国经济增长的一个重要因素。1998年的全球网上营业额已达到1020亿美元。中国互联网起步虽迟却发展神速，互联网用户已达到2250万，电子商务成为热点。2000年国，我国电子商务交易总额为771.6亿元人民币。

电子商务的发展需要一个良好的网络环境，需要网络的安全运作。然而，网络拥有较为复杂的设备和协议，保证复杂的系统没有缺陷和漏洞是不可能的。同时，网络的地域分布使得安全管理难于顾及网络连接的各个角落，没有人能证明网络

是安全的，这便使网络安全问题变成一个风险管理问题，安全性成为概率意义上无法准确定义的指标。于是，黑客便有了可乘之机。

## 揭开黑客神秘面纱

黑客显然是极为出色的编程高手。在20世纪60年代和70年代，做一名计算机黑客是一件很荣耀的事情。在国外，“黑客”在当时用来形容独立思考、然而却奉公守法的计算机迷。他们崇尚技术、反抗权威。他们的骨子里渗透了“英雄”般的反权威思想。从事黑客活动，意味着对计算机系统的最大潜力进行智力上的自由探索，意味着尽可能地使计算机的使用和信息的获得成为免费的和公开的，意味着坚信完美的程序将解放人们的头脑和精神。他们云集在技术精英的堡垒——麻省理工学院和斯坦福大学。作为一个群体，他们的商业意识十分薄弱，政治意识更是匮乏，是一些地地道道的技术人员。

如今，国外许多年轻人从一批诸如“黑客俱乐部”、“黑客基地”等网站上了解到一些黑客手法和工具，使得这些涉世不深、法律意识淡薄，但对计算机系统和网络有着浓厚兴趣的青少年，对侵入他人计算机系统充满了好奇和技术挑战心态。也有一些居心不良，以恶意破坏网络和盗取情报、金钱为目的的犯罪分子混杂其中，从而构成了一个复杂的黑客群体，对计算机系统和信息网络构成了安全威胁。应指出的是，一些被黑客行为扰乱过的计算机系统由于门户洞开，随时可能被真正的犯罪分子乘虚而入。然而，任何不负责任、失去方向和不受制约的权力都是令人恐怖的，计算机系统的控制权也不例外。

随着一些黑客逐渐将注意力集中到涉及大公司商业机密或国家要害部门的保密数据库上，“黑客”的定义有了新的演绎，对国家安全造成的威胁也越来越大。有些国家甚至担心，一旦黑客们利用技术获取国家机密并出售给恐怖主义组织，后果将不堪设想。

1999年，英国媒体曾透露出一条爆炸性的消息说，几十名黑客联手劫持了英国的一颗卫星，并威胁若政府不付出赎金，他们将销毁这颗卫星。尽管这条消息尚未得到证实，但有关专家已表示，这说明“黑客恐怖主义”已发展到了新的阶段。

## 黑客手段日益高超

在最近多起黑客袭击的案例中，黑客们并没有像以前那样入侵到被攻击的网络中窃取信息或涂改网页，他们开始使用一种特别的方法使该网站的服务不可用，这就是拒绝服务攻击。拒绝服务攻击可以使网站服务器充斥大量要求回复的信息，消耗网络带宽或系统资源，导致网络或系统不胜负荷以至于瘫痪而停止提供正常的网络服务。

在1999年8月17日，一个由至少227台主机（其中114台属于Internet2主机）组成的trinoo网络攻击了位于明尼苏达大学的一台主机，其结果是该主机网络崩溃超过两天。而在调查这次攻击期间，又有至少16台其他主机被攻击，其中包括了一些美国以外的主机。这是拒绝服务攻击技术的早期运用。

2000年2月，黑客攻击美国著名网站时，使用的是一种更为先进的分布式的拒绝服务攻击技术。攻击者先是探测扫描大量主机以寻找可入侵主机目标，入侵有安全漏洞的主机并获取控制权；接着在每台入侵主机中安装攻击程序，利用已入侵主机继续进行扫描和入侵。

为了提高分布式拒绝服务攻击的成功率，攻击者需要控制成百上千的被入侵主机。而且由于整个过程是自动化的，攻击者能够在5秒钟内入侵一台主机并安装攻击工具。这样一来，黑客在短短的一个小时内便可以入侵数千台主机。

我们曾经做过这样的比喻，一旦局域网的某台机器被黑客攻破，临近的网上机器由于口令可能被监听，也同样处于危险之中。就像一条街上的邻居被盗贼潜入后，四邻八舍都不得安宁。现在看来，如果一台计算机不采取网络安全措施，它还可能立即被利用为攻击他人的跳板，成为黑客利用分布式拒绝服务技术进行攻击的前哨阵地。目前已经发现，斯坦福大学有几十台计算机曾被利用作此次黑客攻击网站的跳板，令人触目。

## 各国政府重拳出击

随着因特网的普及，网络安全问题越来越重要。据统计，到1999年，全球个人电脑总数达4.4亿

台，因特网使用者达 2.59 亿。到 2005 年全球因特网用户可达到 7.65 亿。此外，基于因特网的电子商务迅速发展，据预测，到 2002 年，全球通过入门网站达成的贸易额将达 5 万亿美元。人们不难想象黑客攻击一旦得逞，小则网络某项服务瘫痪，大则造成短时间内无法恢复的整个网络的瘫痪，造成巨大损失。

时值今日，人们已经深知因特网上的黑客问题是各国网络界极其头疼的问题。在因特网日益渗透到人们工作和生活的今天，提高因特网的防卫能力，保证信息安全已经成为当务之急。

对于网络的安全问题，各国政府纷纷作出反应。美国总统比尔·克林顿召集一批科技专家及一名叫“马奇”的神秘黑客到白宫，商讨加强世界网络安全的办法。这次会议的起初构想是讨论恐怖分子利用电脑网络进行活动的问题。但克林顿表示，上星期的袭击更说明政府有必要集中精力保护互联网。虽然这种“阻断服务”的袭击显然非常令人困扰，但他认为美国有办法使互联网的安全问题得到改善。

2000 年，日本中央机关网站频频遭到黑客的入侵。日本政府决定从 2 月 13 日起实施黑客法、禁止未经授权的电脑网络存取，同时，日本企业也已开始动作，研拟回应黑客的对策，将未经授权的网络存取定义为使用他人的身分及密码侵入电脑网络。若被视为黑客等其他电脑相关犯罪的第一步，未经授权存取将被处以最高一年的徒刑。在未经所有人许可下，交易他人之身分，将被处以最高 30 万日元的罚款。

中国在 1999 年修订《刑法》中，增加了对非法侵入重要领域计算机信息系统行为刑事处罚的明确规定。1997 年，经国务院批准，公安部发布的《计算机网络国际联网安全保护管理办法》中也规定，禁止任何单位和个人，未经允许进入或破坏计算机信息网络。值得一提的是，中国有关加强网络管理规定出台时，曾受到西方一些官员和媒体的非议，现在正是这些国家发生重大的黑客侵网事件，他们只得重新重视“加强网络管理”。

尽管各国对网络管理方式各有不同，但在加强网络监督上有共同目标，就是防止黑客干扰和破坏。

## 中国网络也受威胁

从某种意义上说，由黑客袭击而造成计算机网络系统瘫痪事件是恐怖的，因为信息是 21 世纪的发展支柱，如果有恐怖分子袭击一个国家的核心信息系统，如金融、商贸、交通、通信、军事等系统，以及建立在其上的经济体系，其后果并不亚于用炸弹直接轰炸国家重要设施。

有专家预测，通过网络攻击对手的核心信息系统并使之瘫痪的网络战将成为传统战争之后的一种全新形式的战争，“网军”有可能成为继陆、海、空三军之后的又一新兵种。据报道，科索沃战争中，南联盟的电脑黑客们对北约国家进行了攻击，曾造成白宫和五角大楼的计算机系统被迫中断运行。

专家警告，凭中国网络技术现状，很难抵御黑客们的攻击行为，而且一旦遭到破坏，恢复起来也相当困难。那么，中国各种类别的网站安全系数到底有多大？让我们来看看国内网络的现状。

我国的许多网络在建网初期确实较少或者根本就没有考虑安全防范措施，不少网络工程本身没有认真处理网络系统的安全环节，就像给人家盖楼而没有给门窗配锁就交付使用，是经不起严格验收的。因此，有相当大比例单位的计算机系统或多或少都存在着安全漏洞，随时都有可能遭受黑客袭击。

这一两年许多人开设网站的积极性很高，但网络管理的水平却没有及时跟上。无须多加说明，我国目前极缺网络及电脑高级系统管理人才。由于高等教育尚未专门培养这方面人才，社会上又缺乏造就这类人才的实践环境，像 SUN、IBM、HP、NT 等这类大型服务器的高级系统管理一般人不易接触到。这种人才往往又都是外企重点招聘的对象，导致我国在各网络运行的机构大多缺乏得力可靠的系统管理员，这使许多网络的运行处于低水准，非常不安全。大多数国内的网络提供商（ISP）及从政府到企业的信息提供网站（ICP）还缺乏有经验的安全员，连黑客在网站内筑了窝还蒙在鼓里。有些领导或企业总裁不大了解高技术中的这些情况，既没有选拔可信的技术人员，又没有创造必要的条件保证这些技术人员的稳定和技术上的深造。对这种状态的网络系统必须及早采取措施。

## 结束语

世界上几乎每 20 秒就有一起黑客事件发生，仅

美国每年所造成的经济损失就超过100亿美元。信息化不是一句空话，现代化的战争离不开它，现实社会的经济命脉就在现代信息技术的操纵下搏动。

信息化给一个国家带来希望，也可能带来麻烦。如果信息化不是在靠科学决策，靠高技术队伍，这种"信息化"必然是某些因素误导的结果。可以说一些网络工程安全质量不能保证，是一些商业驱动的结果。我国不成熟的网络市场将使一些网络服务商自行倒闭。某些企业的失败在信息时代不足为奇，而一个国家的信息系统处于不安全的状态，则它的结局将是十分痛苦的。如果不能根本解决诸如黑客入侵这样的网络安全问题，信息产业只能成为信息麻烦。

据中国互联网络信息中心提供的统计数据，目前Windows NT占据国内3700个站点操作系统的91%。不论在系统运行稳定性还是实际的安全性能方面都可说Windows NT不如UNIX操作系统，极容易由于受到黑客的攻击而陷入瘫痪。UNIX的系统虽然所占的比例不高，但都是用在关键部位，如网络域名服务器、电子邮件服务器及数据库等。在政府、电信及金融部门多用UNIX计算机系统，所用机型从SUN、IBM到HP、SGI等。因此集中解决UNIX相关的网络与系统防范黑客入侵问题，成为网络安全研究的一个切入点。黑客入侵一般是：首先利用网络协议的一些漏洞，获取系统的口令文件，然后对口令进行破译，再利用破译后的帐号进入系统。如果进入的帐号为普通用户帐号，他们会利用系统现存的一些漏洞，使用许多工具获得特权，修改系统记录文件。擦掉自己的活动记录，使得安全机制对他们失去作用，然后就开始任意胡作非为。值得一提的是，目前各单位通常所使用的基于路由器的第一代防火墙产品，这类产品只有分组过滤的功能（如IP地址、端口号等），极易被黑客绕过或攻破。何况许多黑客通过电话拨号上网的，他上来就已经在防火墙内了。统计表明多数危险的黑客就是内部人员通过平时上机作案的。

互联网的出现，堪称人类社会一次革命性的变革。如今，互联网技术已被广泛接受。但在享受互联网带给我们种种好处的同时，网络安全却时时困扰着我们。它就像一柄达摩克利斯剑，高悬在互联网络世界的上空，不断地提醒着我们：网络时代，勿忘安全！

解放日报

2001年4月4日

# 信息安全 保密

●中国工程院院士 沈昌祥

信息安全保密是指秘密信息在产生、传输、使用、存储过程中不被泄露或破坏，确保信息的可用性、保密性、完整性和不可否认性，并保证信息系统的可靠性和可控性，是一项复杂的系统工程。当前，最突出的是计算机信息系统的安全保密，它所面临的威胁主要包括：利用网络的开放性，采取病毒和黑客入侵等手段，渗入计算机系统，进行干扰、篡改、窃取或破坏；利用在计算机CPU芯片或在操作系统、数据库管理系统、应用程序中预先安置从事情报收集、受控激发破坏的程序，来破坏系统或搜集和发送敏感信息；利用计算机及其外围设备电磁泄漏，侦截各种情报资料等。

针对威胁，可以把信息安全保密内容分为：实体安全、运行安全、数据安全和管理安全四个方面。实体安全是指保护计算机设备、设施（含网络）以及其它媒体免遭地震、水灾、火灾、有害气体和其它环境事故（如电磁污染等）破坏的措施、过程。运行安全是指为保障系统功能的安全实现，提供一套安全措施，如安全评估、审计跟踪、备份与恢复、应急措施等，来保护信息处理过程的安全。数据安全是指防止信息资源被故意的或偶然的非授权泄漏、更改、破坏，或使信息被非法系统辨识、控制和否认。管理安全是指有关的法律法令和规章制度以及安全管理手段，确保系统安全生存和运营。管理手段是对安全服务和安全机制进行管理，把管理信息分配到有关的安全服务和安全机制中去，并收集与它们的操作有关的信息。

要使信息安全保障系统有足够的保障能力，就必须具有完善的安全服务和机制，如身份鉴别、访问控制、密码加密、完整性校验、防止否认、审计管理、有用控制和应急备份等。使信息系统的攻击者"进不去、窃不走、看不懂、改不了、打不乱、赖不了、跑不掉"，建立起有效的安全屏障。

近些年来，信息安全保密方面出现了一些新概念，如信息安全保障，其内涵已超出传统的信息安全保密，而是保护、检测、反应、恢复的有机结合，称之为PDRR模型。PDRR模型把信息的安全保护作为基础，但信息系统保护是活动过程，要用检测的手段来发现安全漏洞，及时更正；同时应有应急响应措施，以对付各种入侵攻击。另外，还应有快速的恢复功能，使系统受攻击破坏的损失降到最低程度。须知，仅仅依靠政策、法规和保密技术是不够的，还必须建立实体操作。

## 信息安全保密将是21世纪军事对抗的焦点

信息安全保密将是21世纪军事对抗的焦点，是敌对双方借以获取信息优势的制高点。以信息技术为核心的未来军事斗争是一场智力的较量，谁占据了信息安全保密的制高点，谁就掌握了制信息权，也就掌握了信息战中的制胜权。

信息安全保密使军事斗争中的优势与弱势成为相对的概念。

在以信息战为主体的战争中，发达国家与不发达国家的差距远远小于他们在常规战争中的差距。对我国而言，应扬长避短，“有所为，有所不为”，把信息系统安全保密建设提高到“两弹一星”的高度去认识，加大对信息安全保密研究的投入，并借鉴世界先进技术和成功经验，独立自主地构筑信息安全保障体系，抢占信息安全保密制高点，这也是高技术条件下打赢现代战争的“杀手锏”。

目前，我们急需强化信息安全保障体系，确立信息安全战略和防御体系，这既是时代的需要，也是国家安全战略和军队发展的需要，更是现实斗争的需要。

## ●竞相采取应对之策

国际上围绕信息资源的获取、使用和控制的斗争愈演愈烈，各国都把建立牢固的安全保障体系作为基本国策。美国1998年5月发布第63号总统决定令，要求行政部门评估国家关键基础设施的计算机脆弱性，着重强调了要保护政府自身的关键设施免受计算机攻击，对其缺陷进行修正，树立信息安全典范，并要求联邦政府制定保卫国家使其免受计算机破坏的详细计划。紧接着，于2000年1月又以总统决定令发布了《保卫美国计算机空间——信息系统保护国家计划V. 10》。这是一个规划美国计算机安全保护计划持续发展和更新的综合性方案，提出了举国上下团结应战要达到的战略目标。该计划实施将为美国的经济、国家安全、公共安全中的关键部门提供有效的保护措施。美国对世界各国大量倾销计算机等信息产品及系统，并禁止高安全等级的设备出口，在网络信息安全保障上最为先进，处于霸主地位。

俄罗斯对信息安全极为重视，一方面建立国家统一的自主的安全保障体系，制定了“联邦信息安全学说”；另一方面向国际社会提出签订制止信息战的国际和约的建议。日本作为亚洲信息化程度最高的国家，十分重视自己信息安全保障体系的强化，早在20世纪90年代初就开发了自主操作系统内核和选用网络时代的密码算法，构筑牢固的信息安全保护屏障。

目前美国微软的操作系统和办公系统软件已占据我国90%的份额，从不断发现的软硬件“后门”看，攻击者完全有能力植入遥控机制，一旦触发，可能导致系统全面瘫痪。信息安全保密解决不好，将直接威胁国家和民族的安危。因此，国家应该把信息安全保障作为战略决策，加大经费投入力度，严密组织科研攻关，使信息安全保密建设取得实质性进展，构筑我国信息与网络安全防线。

解放日报

2001年4月18日

★信息安全系列谈（3）

# 防不胜防的通信泄密

●姚明 邵飞林

## ·通信信道：主要的泄密渠道

通信泄密在信道和终端都可能发生，但最常见、最直接的威胁是对信道进行侦听。众所周知，信号传播常用的方式有电缆传播、无线电波传播和光缆传播。对于电缆传播方式，可以采用感应式窃听器拾取信号。一家美国媒体最近披露，20世纪70年代早期，美国海军“哈利伯特”潜艇上的潜水员，在前苏联领海纵深内部的鄂霍次克海120米深的海底军事通信电缆上安装了一个6米长的窃听设备，这个窃听设备记录下所有经过电缆的通信信号。由于前苏联军队没有对通信电缆采取任何加密措施，因此大量军事通信情报就这样轻易地被美国人掌握了。

无线电通信，信号直接在广阔的空间传播，泄密的威胁更大。例如：一部超短波电台发出的信号可覆盖直径数十公里的地面；一部中等功率的短波电台发出的信号可以在地面和电离层之间多次反射，传送到数千公里以外的地方；而一颗地球同步卫星发出的信号可以覆盖全球1/3的面积。在无线电波有效的范围内，无论

在地面还是天空，只要采用适当的接收设备就可以进行侦听。冷战时期，美国国防部下属机构——国家安全局建立了一个代号为“梯形队”的覆盖全球通讯间谍网络，该网络每年耗资 8 亿美元，在全球有 15000 个工作人员操纵它的运转。在宇宙空间，它能管辖 120 颗卫星，不停地监视着地面；在地面它有两个重要的处理中心，一个在美国，一个在英国。此外，在加拿大、新西兰和澳大利亚还有数十个大型接收站，每个接收站的规模都相当庞大，在英国北约克郡荒漠上的一个接收站面积就有 30 个高尔夫球场那么大，巨大的接收装置在数英里外就能看见。它不仅用于窃取敌对国家的军事机密，也用于收集盟国的经济情报，使美国在竞争中处于有利地位。欧洲议会估计，由于“梯形队”的窃听行为，欧盟各国至少因泄密损失了 200 亿欧元。

光缆通信是依靠光缆内部的光信号进行通信的，由于没有电磁辐射，要在外部进行窃听技术上十分困难，但如果在光缆上接入光分支器将光信号引出并进行窃听，在技术上也是可以实现的，因此，光缆通信同样存在泄密的可能。

## 信息加密：难保万无一失

1941 年 1 月，美军击沉了日军“伊－124”号潜艇，并在潜艇内找到了日本海军最高密级的“JN－25B”密码本，意外的收获使美军大大加快了破译密码的工作。很快，美军又进一步破译了日军中途岛战役的作战部署，使美日双方的军事力量发生了根本的变化。事后，尼米兹将军说：“美军破译了日军的密码电报，所以完全掌握了日军的作战计划，美国的胜利才成为可能。对付日本的威胁，美国海军兵力实在相差太远了，破译这个情报，使美军指挥官避免了一场灾难。”

近 20 年来，随着信息技术的飞速发展，密码研究队伍已从传统的纯军事领域扩展到社会各界，刺激着密码破译理论和手段取得巨大的进步。特别是因特网的发展，使密码破译可以充分利用全网的资源，对一种密码进行合力攻关。而且，发达国家的计算能力每一年半就提高一倍，使密码的生存期大为缩短，给信息安全造成了极大的威胁。

## 电磁波散射：主要安全威胁

破译密码通常需要大量的人力、物力和时间。实际上，采用无线电侦察监测技术，无需破译密码也可以发现隐藏在信号背后的秘密。例如，无线电信号很容易泄露电台的数量、位置，电台功率的大小、工作的时间等参数，采用无线电接收机、信号分析仪和测向设备，侦收、分析所得的参数就可以判断对方的兵力部署和可能的军事行动。为了对付无线电侦察，一般可以采用无线电静默和无线电佯动，使敌方失去目标或不能进行正确的判断。

随着技术的发展，通信保密与技术窃密的斗争，将不断升级，永无停息。我们只有在保证通信畅通的同时，采取有效的措施确保通信安全保密，才能在经济、政治和军事斗争中立于不败之地。