网络生活

Internet

100问 网络安全

2

初 英／编著

序

随着社会的发展和人类的进步，计算机已经普及到了几乎每一个办公室和大部分的家庭，计算机和网络已经触及到人们生活的每一个角落。怎样收发电子邮件，如何在家中上网，怎样在网上购物和炒股，这些曾经看起来离普通老百姓遥不可及的事情，现在已经成了我们生活中不可缺少的一部分。

但是计算机和网络方面的书籍在普通人眼里仍然是一些高深莫测的专家的教诲，是需要花费许多钱才能买回来，花很多时间才能看懂的东西。虽然有很多打着“入门”、“傻瓜”名义的图书，但是很多却是从国外翻译的，或者只是软件的说明书。能从用户的角度来考虑问题，及时回答用户的各种问题的书籍还不多。

本套丛书就是从用户的角度，以问答方式来解决用户的各种问题，特别是关于网络的问题。短小、实用、便宜是它的三大特色。虽然其中还有一些不足，例如：问题的分类还不准确，问题的提炼还不

很精炼，但是这是我们见到的比较精彩的一套网络知识丛书。特别是“网络安全一百问”，无论对于网络的初学者，还是有一定网络知识的用户，都有一定的借鉴意义。

希望这本书能对网络知识的普及，使广大群众摆脱对网络的神秘感有一定的帮助。

中国国家信息
安全测评认证中心主任
吴世忠

2000 年 7 月 12 日

目　录

一、网络安全简介

1. 什么是网络安全？

“上网”可以说是这两年最热门的一个词，无数篇报导都在鼓动人们去“上网”，种种报道都说网上的世界很精彩，人们可以上网看报纸、听音乐、玩游戏，可以实现网上采购、逛商店、买股票，甚至还可以上网络银行。但也有反面的报导，例如：网络中的黄色站点、网络黑客、网络病毒等等。

因此，当人们在网络上与外界相连时，很多人都会产生同一个问题：网络安全吗？

网络安全是一个很复杂的问题，具体含义会随着“角度”的变化而变化。比如：从用户（个人、企业等）的角度来说，他们希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护，避免其他人或对手利用窃听、冒充、篡改、抵赖等手段侵犯用户的利益和隐私，同时也避免其它用户的非授权访问和破坏。在进行网

上购物时，能否保证自己的密码、银行帐号不被其他人窃取等。

从网络运行和管理者角度说，他们希望对本地网络信息的访问、读写等操作受到保护和控制，避免出现。病毒、非法存取、拒绝服务和网络资源非法占用和非法控制等威胁，制止和防御网络黑客的攻击。

对安全保密部门来说，他们希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵，避免机要信息泄露，避免对社会产生危害，对国家造成巨大损失。

从社会教育和意识形态角度来讲，网络上不健康的内容，会对社会的稳定和人类的发展造成阻碍，必须对其进行控制。

从国家的方面来讲，网络安全是一个关系国家安全和主权、社会的稳定、民族文化的继承和发扬的重要问题。其重要性，正随着全球信息化步伐的加快而变得越来越重要。“家门就是国门”，安全问题刻不容缓。

网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

网络安全从其本质上来讲就是网络上的信息安全。从广义来说，凡是涉及到网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。

2. 为什么要研究网络的安全问题？

随着计算机技术的飞速发展，信息网络已经成为社会发展的重要保证。信息网络涉及到国家的政府、军事、文教等诸多领域。其中有许多是政府宏观调控决策、商业经济信息、银行资金转帐、股票证券、能源资源数据、科研数据等重要信息。有很多是敏感信息，甚至是国家机密。所以难免会吸引来自世界各地的各种人为攻击（例如信息泄漏、信息窃取、数据篡改、数据删添、计算机病毒等）。同时，网络环境还要经受诸如水灾、火灾、地震、电磁辐射等方面的考验。

近年来，计算机犯罪案件也急剧上升，计算机犯罪已经成为普遍的国际性问题。据美国联邦调查

局的报告，计算机犯罪是商业犯罪中最大的犯罪类型之一，每笔犯罪的平均金额为45000美元，每年计算机犯罪造成的经济损失高达50亿美元。

计算机犯罪大都具有瞬时性、广域性、专业性、时空分离性等特点。通常计算机犯罪很少留下犯罪证据，这大大刺激了计算机高技术犯罪案件的发生。

计算机犯罪率的迅速增加，使各国的网络系统面临着很大的威胁，并成为严重的社会问题之一。

3. 能介绍一些网络安全案例吗？

关于网络攻击的案例有很多。

1996年初，据美国旧金山的计算机安全协会与联邦调查局的一次联合调查统计，有53%的企业受到过计算机病毒的侵害，42%的企业的计算机系统在过去的12个月被非法使用过。而五角大楼的一个研究小组称美国一年中遭受的攻击就达25万次之多。

1994年末，俄罗斯黑客弗拉基米尔·利文与其伙伴从圣彼得堡的一家小软件公司的联网计算机上，向美国CITY BANK银行发动了一连串攻击，通过电子转帐方式，从CITYBANK银行在纽约的计算机主机里窃取1100万美元。

1996 年 8 月 17 日，美国司法部的网络服务器遭到黑客入侵，并将“美国司法部”的主页改为“美国不公正部”，将司法部部长的照片换成了阿道夫·希特勒，将司法部徽章换成了纳粹党徽，并加上一幅色情女郎的图片作为所谓司法部部长的助手。此外还留下了很多攻击美国司法政策的文字。

1996 年 9 月 18 日，黑客又光顾美国中央情报局的网络服务器，将其主页由“中央情报局”改为“中央愚蠢局”。

1996 年 12 月 29 日，黑客侵入美国空军的全球网网址并将其主页肆意改动，其中有关空军介绍、新闻发布等内容被替换成一段简短的黄色录象，且声称美国政府所说的一切都是谎言。迫使美国国防部一度关闭了其他 80 多个军方网址。

1999 年 3 月，当美国开始轰炸南斯拉夫时，南斯拉夫的计算机高手就开始对美国和欧盟的站点攻击，曾经使很多站点陷入瘫痪。

2000 年 2 月，一群网络少年黑客，采用最简单的技术对 yahoo, aol, msn, ebay 等世界上最著名的网站进行了共计，而我国的 sina 等受到了攻击，从而再一次证明了网络的脆弱性。

4. 我国也有计算机安全问题吗？

应该说，我国的网络水平还不高，因此，网络管理、安全防护的技术都存在一些漏洞，因此更容易受到攻击，例如：

1996年2月，刚开通不久的Chinanet受到攻击，且攻击得逞。

1997年初，北京某ISP被黑客成功侵入，并在清华大学“水木清华”BBS站的“黑客与解密”讨论区张贴有关如何免费通过该ISP进入Internet的文章。

1997年4月23日，美国得克萨斯州内查德逊地区西南贝尔互联网络公司的某个PPP用户侵入中国互联网络信息中心的服务器，破译该系统的shutdown帐户，把中国互联网信息中心的主页换成了一个笑嘻嘻的骷髅头。

1996年初CHINANET受到某高校的一个研究生的攻击；1996年秋，北京某ISP和它的用户发生了一些矛盾，此用户便攻击该ISP的服务器，致使服务中断了数小时。

从1998年开始，由于用户水平的不断提高，站点的不断增多，关于网络攻击方面的报导也越来越

多，其中国内最重要的两次黑客事件是：

1999 年 5 月，美国飞机轰炸中国驻南斯拉夫大使馆，中国的黑客对美国、欧洲的许多站点进行了攻击，修改了很多站点的网页。

从 1999 年 8 月开始，台湾海峡两边的计算机高手开始了互相之间的攻击，两岸的很多站点都被攻破。

5. 网络安全包括哪些方面？

从技术上来讲，网络安全包括以下方面：

运行系统安全，即保证信息处理和传输系统的安全。它侧重于保证系统正常运行，避免因为系统的崩溃和损坏而对系统存贮、处理和传输的信息造成破坏和损失，避免由于电磁泄漏，产生信息泄露，干扰他人，受他人干扰。

网络上系统信息的安全。包括用户口令鉴别，用户存取权限控制，数据存取权限、方式控制，安全审计，安全问题跟踪，计算机病毒防治，数据加密。

网络上信息传播安全，即信息传播后果的安全，包括信息过滤等。它侧重于防止和控制非法、有害的信息进行传播后的后果。避免公用网络上大量自

由传输的信息失控。

网络上信息内容的安全。它侧重于保护信息的保密性、真实性和完整性。避免攻击者利用系统的安全漏洞进行窃听、冒充、诈骗等有损于合法用户的行为。本质上是保护用户的利益和隐私。

6. 网络安全有什么特征？

网络安全应具有以下四个方面的特征：

保密性：信息不泄露给非授权用户、实体或过程，或供其利用的特性。

完整性：数据未经授权不能进行改变的特性。即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性。

可用性：可被授权实体访问并按需求使用的特性。即当需要时能否存取所需的信息。例如网络环境下拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击。

可控性：对信息的传播及内容具有控制能力。

7. 网络安全分成几个结构层次？

自然灾害（如雷电、地震、火灾等），物理损坏（如硬盘损坏、设备使用寿命到期等），设备故障（如

停电、电磁干扰等），意外事故。解决方案是：防护措施，安全制度，数据备份等。

电磁泄漏，信息泄漏，干扰他人，受他人干扰，乘机而入（如进入安全进程后半途离开），痕迹泄露（如口令密钥等保管不善）。解决方案是：辐射防护，屏幕口令，隐藏销毁等。

操作失误（如删除文件，格式化硬盘，线路拆除等），意外疏漏。解决方案是：状态检测，报警确认，应急恢复等。

计算机系统机房环境的安全。特点是：可控性强，损失也大。解决方案：加强机房管理，运行管理，安全组织和人事管理。

8. 对网络可能产生危害的因素有哪些？

自然灾害、意外事故；

计算机犯罪；

人为行为，比如使用不当，安全意识差等；

“黑客”行为：由于黑客的入侵或侵扰，比如非法访问、拒绝服务计算机病毒、非法连接等；

内部泄密；

外部泄密；

信息丢失；