★ 信息安全丛书　国家十五规划重点图书

★ 国家863计划信息安全技术发展战略研究专家组

★ 中国信息安全产品测评认证中心

信息安全技术基础和安全策略

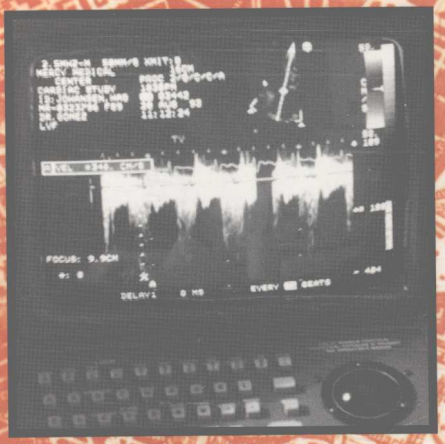
XINXIANQUAN

JISHUJICHUHE

ANQUAN

CELUE

薛　质　李建华　诸鸿文/编著



贵州科技出版社

信息安全技术基础和安全策略

XINXIANQUAN JISHUJICHUHE ANQUAN CELUE

薛 质 李建华 诸鸿文/编著

贵州科技出版社

图书在版编目(CIP)数据

信息安全技术基础和安全策略/薛质,李建华,诸鸿文编著.—贵阳:贵州科技出版社,2005.3
(信息安全丛书/何德全主编)
ISBN 7-80662-112-1

Ⅰ.信… Ⅱ.①薛…②李…③诸… Ⅲ.计算机网络—安全技术 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2005)第 014116 号

贵州科技出版社出版发行
贵阳市中华北路 289 号
邮政编码:550004
印　　刷:贵州云商印务有限公司
经　　销:贵州省新华书店
760 mm×1 092 mm　16 开本　18.875 印张　450 千字
2005 年 3 月第 1 版　第 1 次印刷
定　　价:40.00 元

《信息安全丛书》编著单位

国家863计划信息安全技术发展战略研究专家组

中国信息安全产品测评认证中心

《信息安全丛书》编辑委员会

总　序

人类社会进入21世纪，以互联网为标志的信息时代的社会轮廓日益明晰。在这个新时代所蕴育的新世界里，人、网、环境相耦合构成了一个复杂巨系统。通过互联网的协同交流，人的智能和计算机的运算能力融合重构，涌现出社会生产力发展的崭新内涵，极大地提高了人类和环境协调发展的能力，同时，也深刻地改变着人类自身经济、社会、文化的结构和运行方式。

正如马克思所说，人的本质是“一切社会关系的总和”。在这个复杂巨系统中，“人”以资源使用者的身份出现，是系统的主体，处于主导地位。而系统资源（包括通讯网络、计算机软件与硬件、数据和信息内容等）则是客体，它是为主体即“人”服务的。与此相适应，信息安全的主体也是“人”，其目的主要是保证主体对网络资源的控制。由些可见，提高“人”的信息安全意识，加强“人”的信息安全教育，已成为我们开展信息安全工作、构建信息安全保障体系的关键问题。

在国家科技部的直接领导下，在社会各界的大力支持下，我们在开展国家863计划信息安全技术应急项目、国家信息安全应用示范工程（上海S219工程）、国家信息安全产业化基地建设等项工作的同时，组织编写了这套《信息安全丛书》，力图集成国内信息安全专家们的智慧，较为全面地阐释多年来从事信息安全理论与实践工作的体会。

丛书的编写得到了天虹信科技咨询中心、中国科学院信息安全国家重点实验室、天融信网络安全技术有限公司、启明星辰信息技术有限公司、北京江南科友科技有限公司等社会各界的大力支持与帮助，并被国家新闻出版总署列入“十五”国家重点图书出版规划，在此谨对各位作者及各个方面的努力表示衷心感谢。

信息安全是一个蓬勃发展的新兴领域，本套丛书的缺点和不足在所难免，希望大家多提宝贵意见，与时俱进，共同为提高全民族的信息安全意识，推动我国信息安全科技发展，促进我国信息安全保障体系建设作出贡献。

编　者

2004年5月

前　言

计算机网络(以下简称网络)近几年在我国有了很快的发展。在网络的大量应用中,安全正面临着前所未有的挑战。信息安全已经成为一个综合性工程,甚至将成为一个新兴的研究学科,它需要我们在网络安全领域进行长期的研究和攻关。

网络的基础在于资源的共享。自由,一直以来是网络的基本准则。随着Internet的迅速发展,网络上的资源共享越来越强化,随之而来的,是网络安全问题越来越突出。

目前,Internet已遍及世界240个国家和地区,每时每刻都为用户提供各种类型的信息服务。随着技术的飞速发展,Internet的服务已经日益呈现出多样化的特征,除了最初的电子邮件、WWW外,越来越多的集合视频、声音、数据于一体的服务在Internet出现了,如:视频会议、网络电话等。

现在的社会是高度信息化的社会,计算机已经被应用到政治、军事、金融、商业、交通、电信、教育等各个行业。人们在日常的生活中对计算机的依赖程度大大提高了,尤其是近年来国家实施的信息系统工程和信息基础设施建设,已经使计算机信息系统成为当今社会特征的一个重要组成部分。越来越多的各类信息管理系统,收集和储存了大量的个人私密资料和信息,而这些信息的处理和交换大多通过网络来完成。毫不夸张地说,网络已经成为人们获取信息的一个重要途径,正日益改变着人们的生活方式。随着网络的不断发展,网络的资源共享性、开放性、交换性日益增强,各种原来不可能实现的业务都在网络上出现了。电子货币、数字签名、电子商务、政务上网、网络银行,使得人们可以在家中完成"一切"的交易。各类银行网络的建设,更是使资金的异地流通变得快捷方便了。这一切也随之带来了巨大的安全隐患和风险。

计算机犯罪已经成为一种新的高智能犯罪,它具有高度的隐蔽性,给社会带来了巨大的危害,也给侦破工作带来了一定的麻烦。同时,由于网络的广泛互连和无地域性特征,使得计算机犯罪可以轻松地实现异地甚至是跨国的犯罪和资金转移。

"黑客"——一个神秘的带着传奇色彩的称呼,他们像是网络世界中的"侠客",凭借着高超的技术在网络世界自由驰骋,几乎没有什么可以阻拦他们,他们崇尚高度的、绝对的自由。据调查,有60%以上的青少年网络用户梦想成为一个"黑

客”。在信息高度发展的美国，重要部门的计算机信息系统每天都发生着大量的入侵事件，造成了上亿美元的经济损失。通过计算机盗取信用卡、修改学习成绩、篡改主页，已经是很平常的事情了。

在我国，仅1998年报道的黑客事件就不下5起，大量的网站页面被修改，工作人员的口令和账户被窃取。由于网络入侵的隐蔽性，还有很多的入侵至今没有被发现。有的入侵即使被发现了，出于诸多原因，受害方也不愿意对外宣称。据有关部门统计，利用网络窃取商业机密的事件正以每个月260%的速度增加着。而专家估计，公开报道的入侵事件大约只占入侵事件的0.2%。

“在网络上，没有人知道你是一条狗”，这是一幅漫画上的说明文字，它反映了网络的不可信原则。在网络上，即使是一封非常明白的来信，也极有可能是伪造的。网络安全，已经成为一个最受关注和最时髦的话题，它已不仅是学术研究者的研究方向，而成为全球Internet用户所关注的热点。

多年来，黑客对计算机信息系统的攻击一直没有停止过，其手段也越来越高明，从最初的猜测用户口令、利用计算机软件缺陷，发展到现在的通过操作系统源代码分析操作系统漏洞。同时我们还发现，网络的普及使得攻击工具和代码更容易被一般用户获得，这无疑给网络安全带来了更大的挑战。

解决网络安全问题，任重而道远。

本书内容由浅入深，介绍了网络安全和计算机信息系统安全的相关知识，使读者可以了解中国计算机信息系统的安全现状、网络安全方面的隐患和风险来源、风险给计算机信息系统运行带来的危害以及具体的安全防护措施和技术。

本书中部分内容涉及网络结构、网络协议等知识点，要求读者具备基本的网络操作技能和对网络结构及网络协议的基本了解。

目 录

目　录

1 信息安全概述

信息一直以来都是全人类的宝贵资源。各种功能的信息系统，已经成为推动社会发展前进的催化剂和加速器。同时，由于计算机网络（以下简称网络）的快速普及，处理信息的多样性也使得计算机成为人类社会中一个不可缺少的工具，正日益为社会各个行业和部门的生产和管理提供有效的帮助，其提供的多种信息服务，给人类生活带来了便捷的生活方式。例如与我们关系密切的金融业的信息化进程，使资金流动加快，清算资料的速度大大提高，异地的资金划转也变得十分快捷了。可以这么说，信息化和网络把人和人、国和国的距离缩小了。

信息与信息系统的安全现已成为一个新兴的学科，信息安全管理已经成为公共安全的重要组成部分。信息安全是一个涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学等多种学科的边缘学科。随着全球信息化的发展，国家之间的“距离”越来越小，网络在带来了众多快捷、便利的服务的同时也带来了新的危害。如何解决信息安全问题？如何制止计算机犯罪？如何建立安全的网络体系？这些问题已经成为全球关注的焦点。解决信息安全问题，已经是迫在眉睫的事情了。

网络的安全措施一般分为3类：逻辑上的、物理上的和政策上的。面对安全的种种威胁，仅仅依靠物理上的和政策（法律）上的手段有效防止计算机犯罪显得十分有限和困难，因此必须使用逻辑上的措施，即研究开发有效的网络安全技术，如安全协议、密码技术、数字签名、防火墙、安全管理、安全审计等，以防止网络上传输的信息被非法窃取、篡改、伪造，保证其完整性和保密性；防止非法用户（程序）的侵入，限制网络上用户（程序）的访问权限，保证信息存放的私有性。除此之外，一个安全的网络还必须考虑通信双方的身份真实性和信息的可用性。

网络安全就是要保证网络上存储和传输信息的安全性。由于网络设计之初，只考虑了方便性和开放性，这使得网络非常脆弱，容易受到黑客的攻击或有组织的入

侵，也会由于系统内部人员的不规范操作和恶意破坏，使网络信息系统遭受破坏，信息泄露或丢失。为了解决这些问题，国内外的研究机构在这方面做了很多的工作，在数据加密技术、身份认证、数字签名、防火墙、安全审计、安全管理、安全内核、安全协议、IC卡（存储、加密、智能卡）、拒绝服务、入侵检测、网络安全性分析、信息内容安全监测和信息安全标准化等方面做了大量的研究和开发。

1.1 什么是信息安全

广泛意义上的信息安全是指防止信息财产被故意的或偶然的非法授权泄露、更改、破坏，或防止信息被非法辨识、控制。即确保信息的保密性、可用性、完整性、可控性。信息安全包括操作系统安全、数据库安全、网络安全、计算机病毒防护、访问控制、加密与鉴别等7个方面。

狭义的信息安全指网络上的信息安全，也称为网络安全，它所涉及的领域是相当广泛的。简单地说，网络中的安全指的是一种能够识别和消除不安全因素的能力。

信息安全的定义随着应用环境的改变也有不同的诠释。对用户来说，个人隐私和机密数据的传输受到机密性、完整性和安全性的保护，避免他人窃取资料是他们的安全要求。而对安全保密部门来说，过滤非法、有害或涉及国家机密的信息，成为其信息安全的重点。在下面的相关内容中，我们将对信息安全的具体表现做进一步的说明。

网络安全和其保护的信息对象有关，本质是在信息的安全期内保证其在网络上流动或静态存放时不被非授权用户非法访问，但允许授权用户访问。显然，网络安全、信息安全和系统安全的研究领域是相互交错和联系的。

1.2 网络安全和黑客

一直以来，黑客是具有传奇色彩的崇尚自由的一群人，然而黑客行为造成的损失却是高昂的。据CERT（计算机紧急事件响应小组）的调查显示，约20%的网站都遭受过安全侵害，在美国每年由网络安全事件导致的损失可达100亿美元。根据有关调查，大部分的网络入侵和安全事件的威胁并非来源于外部，而是来源于网络内部的破坏。虽然网络安全已经被全球所重视，各大公司、机构也都纷纷建立了自己的信息安全策略，设置并使用了防火墙、入侵检测系统（IDS）以及跟踪和记录网络活

动的程序，但仍然不足以阻止攻击的产生。原因在于黑客的攻击比起前几年来越来越复杂，技术上越来越先进；超负荷的IT技术人员和由于侥幸心理所导致的资金投入的缺口，使得专业安全技术人员不能获得更多的资源；最重要的一点是没有严密安全保护的计算机信息系统正在全球被大量的快速部署和投入使用。

黑客的分类有很多种标准，一般我们以黑客的行为态度和动机来划分，有以下3类：

(1)偶然的破坏者。顾名思义，这类人喜欢进入他人的计算机信息系统，但不一定有明确目标，多数情况下是恶作剧。大部分黑客属于这一类。

(2)坚定的破坏者。这类黑客的入侵行为带有明确的目标，并会给计算机信息系统带来巨大的甚至是毁灭性的破坏。

(3)间谍。这类黑客窃取商业资料或情报，获得信息或摧毁服务，对资源不加限制地访问。

1.3 计算机信息系统面临的安全威胁、攻击及其脆弱性

网络所提供的资源共享性、用户使用的方便性、分布处理提高效率的特性以及可扩充性，在一定程度上大大增加了网络受攻击的可能性。现今的网络面临着各式各样的安全威胁和人为攻击，而计算机信息系统本身，无论是在存、取运行的基本原理上，或者是系统本身的设计、技术、结构、工艺等方面都存在着一些有待完善的缺陷。或者可以这样说，计算机信息系统本身的脆弱性，使其成为被攻击的目标或被利用为有效的攻击手段。

1.3.1 计算机信息系统面临的安全威胁

计算机信息系统面临的安全威胁来自众多方面，或者说，计算机信息系统本身的脆弱性，使其成为被攻击的目标。计算机信息系统面临的安全威胁可导致信息的保密性、完整性、可用性降低，从而造成经济损失。当前计算机信息系统面临的安全威胁主要有以下方面：

(1)自然灾害、意外事故。由于自然灾害和人为的事故造成的威胁，如天灾、硬件故障、工作人员误操作等。

(2)计算机犯罪。指利用暴力或非暴力，故意破坏计算机中的机密信息，以及危

害计算机实体和信息安全的不法行为，如数据欺骗、特洛伊木马等。

(3)黑客行为。黑客的入侵或干扰，比如非法访问、拒绝服务等。

(4)内部破坏。指内部人员对计算机信息系统的破坏或泄密。

(5)电子情报。通过信息窃取、流量分析、监听等手段获取信息资源。

(6)信息战。为了军事目的，获取或干扰他国的信息和信息系统。

(7)计算机病毒。制造、传播和利用计算机病毒进行破坏计算机信息系统的行为，如常见的蠕虫病毒(求职信、红色代码等)。需要特别注意的是，现在的很多计算机病毒已经具备部分黑客软件的特征。

1.3.2 计算机信息系统受到的攻击

对信息的人为故意的威胁称为攻击。攻击按威胁和攻击的对象可分为两类：一类是对计算机信息系统实体的威胁和攻击；另一类是对信息的威胁和攻击。计算机犯罪和计算机病毒则包括了对计算机信息系统实体和信息两个方面的威胁和攻击。

对计算机信息系统实体的威胁和攻击主要指对计算机及其外部设备和网络的威胁和攻击。对信息系统实体的威胁和攻击不仅会造成财产损失，还会使信息系统遭受破坏。

对信息的威胁和攻击主要有两种：

(1)信息泄露。指偶然的或故意的获得(窃取或分析破译)目标系统的信息，特别是敏感信息。

(2)信息破坏。指由于偶然事故或人为破坏，使信息的正确性、完整性和可用性受到破坏，使系统的信息被修改、删除、添加、伪造或非法复制，造成大量信息的破坏、修改或丢失。

就攻击方式来说，攻击可归纳为主动攻击和被动攻击两类。

被动攻击指一切窃密的攻击。被动攻击是在不干扰系统正常工作的情况下进行侦收、截获、窃取系统信息，以便破译分析；利用观察信息、控制信息的内容来获得目标系统的设置、身份；利用研究机密信息的长度和传递的频度获得信息的性质。被动攻击不容易被用户发现，因此它的攻击持续性和危害性都很大。被动攻击的主要方法有：截获信息、合法窃取、破译分析等。

主动攻击是指篡改信息的攻击。它不仅是窃密，而且威胁到信息的完整性和可

靠性。主动攻击是以各种方式，有选择地修改、删除、增加、伪造、复制信息内容，造成信息破坏。主动攻击的主要方法有：非法冒充、恶意篡改、抵赖等。

1.3.3 计算机信息系统的脆弱性

计算机信息系统本身也存在着一些脆弱性，使得计算机信息系统对安全威胁和攻击的抵御能力很弱，自身的一些缺陷常被非授权用户利用。这种非法的访问不仅使系统中存储的信息完整性受到威胁，使信息被修改或破坏而不能继续使用，更为严重的是，系统中有价值的信息被非法篡改、伪造、窃取或删除而不留一点痕迹。另外，计算机还容易受各种自然灾害和误操作的破坏。认识到计算机信息系统的这种脆弱性，才可以找出有效的措施来保证计算机信息系统的安全。

1.3.3.1 信息处理环节中存在的不安全因素

计算机信息系统的脆弱性，首先从信息的处理环节来看，存在以下的不安全因素：输入数据易被篡改或伪造、系统软件易被破坏、存取控制功能比较弱等。

1.3.3.2 计算机信息系统自身的脆弱性

从计算机信息系统的体系结构方面分析，也存在一些缺陷，包括计算机操作系统的脆弱性、计算机网络系统的脆弱性（包括网络模型、协议上的缺陷）、数据库管理系统的脆弱性等。这些缺陷在短时间内还无法彻底解决。

这些脆弱性将在本书的后续相关内容中详细介绍。

1.4 网络安全的相对性

由于网络的连通性，网络安全不可能达到100%的安全。在制定安全策略限制非法用户访问的同时，也必须保证合法用户对数据的访问权。一般的原则是给用户能足以完成其合法工作的最小权限。那么如何制定安全策略？制定安全策略的原则是什么？一个关键的安全原则应该是实用有效的，同时是不会给合法用户在获取合法信息时增加负担的方案。寻找一个合适安全原则的过程实际上是一个寻求动态平衡点的行为。使用过于复杂的安全技术会使得合法用户的活动大大受限，从而厌烦和规避安全协议。而黑客则随时准备利用这样一个看上去无害的行为。因此，拥有一个过分复杂的安全策略将导致安全有效性的降低。在制定安全策略的时候，总是需要考虑安全策略给合法用户带来的影响。在多数情况下，如果用户所感受到的不

方便大于所产生的安全提高，则该策略实际上降低了网络的安全有效性。

需要指出的是，无论采取何种防范措施都不可能保证网络通信系统的绝对安全。安全是相对的，不安全才是绝对的。在具体实施过程中，经济因素和时间因素是判别安全性的重要指标。换句话说，过时的“成功”攻击和“赔本”的攻击都被认为是无效的。

1.5 网络安全的领域和关键技术

随着信息社会的网络化，越来越多的部门和机构依赖于网络，网络安全的地位日趋重要，一门研究网络安全的学科——信息安全学也开始逐步形成。信息安全学的研究内容主要包括以下方面：

- 网络安全体系结构。
- 网络的攻击手段与防范措施。
- 网络安全设计。
- 网络安全标准的制定和安全评测及认证。
- 网络安全设备。
- 安全管理及安全审计。
- 网络犯罪侦查。
- 网络安全理论与政策。
- 网络安全教育。
- 网络安全法律法规。

明确了网络安全的概念后，我们来讨论网络安全的主要组成和关键性技术。网络安全的结构层次包括：物理安全、安全控制和安全服务。

1.5.1 物理安全

网络安全首先要保障网络上设备的物理安全。物理安全指物理层次上的安全保护。目前主要的物理不安全因素有4类：

(1)自然灾害(如雷电、地震、火灾、水灾等)、物理损坏(如硬盘物理损坏、设备意外损坏等)、设备故障(如意外断电、电磁干扰等)和意外事故。这类风险的特点是：突发性、自然因素性和非针对性。这种安全威胁只破坏信息的完整性和可用性(对信息的

保密性无损害)。对该类威胁的防范一般是实施防护措施,建立数据备份和安全制度。

(2)电磁泄漏(如侦听计算机操作过程)产生信息泄漏、干扰他人、受他人干扰、乘机而入和痕迹泄漏等。其特点是难以觉察性、人为实施的故意性、信息的无意泄漏性。这种威胁只破坏信息的保密性(无损信息的完整性和可用性),解决方法一般是辐射防护、口令和隐藏销毁。

(3)操作失误(如删除文件、格式化硬盘等)或意外疏漏(如系统崩溃等)。其特点是人为实施的无意性、非针对性。这种安全威胁只破坏信息的完整性和可用性(无损信息的保密性),通常用状态检测、报警确认和应急恢复等方法处理。

(4)计算机机房的环境安全。其特点是可控性强,损失大,可管理性强。解决方法是加强计算机机房管理、运行管理、安全组织和人事管理。

物理安全是信息安全的最基本保障,是不可缺少的组成部分。一方面,研制生产计算机和通信设备的厂商应该在各种软件和硬件系统上充分考虑到系统所承受的安全威胁和相应的防护措施,提高系统的可靠性。另一方面,也应该通过安全意识的提高、安全制度的完善、安全操作的提倡等方式使用户和管理维护人员在系统和物理层次上实现信息的保护。

1.5.2 安全控制

安全控制是指通过计算机操作系统和网络通信设备对存储和传输的信息的操作和进程进行控制和管理,主要是在信息处理层次上对信息进行安全保护。可分为3个层次:

(1)计算机操作系统的安全控制。如,用户开机必须输入口令或者指纹等生物特征,以此控制文件的读写存取。主要是保护存储在硬盘上的信息和数据。

(2)网络接口模块的安全控制。在网络环境中对来自其他机器的网络通信进程进行安全控制。包括:身份认证、客户权限设置和识别、审计日志等。

(3)网络互连设备的安全控制。对整个子网内的所有主机的传输信息和运行状态进行安全控制。主要是通过网络管理软件或路由配置来实现。

安全控制主要是通过现有的操作系统和网络管理软件来实现。安全控制只提供初步的安全功能和信息保护,它仍然存在很多的问题,但由于实际情况的限制,很难对此进行弥补和更改。为此,很多科研机构和企业正在研制专门的信息系统安全综合管理软件来实现安全控制。