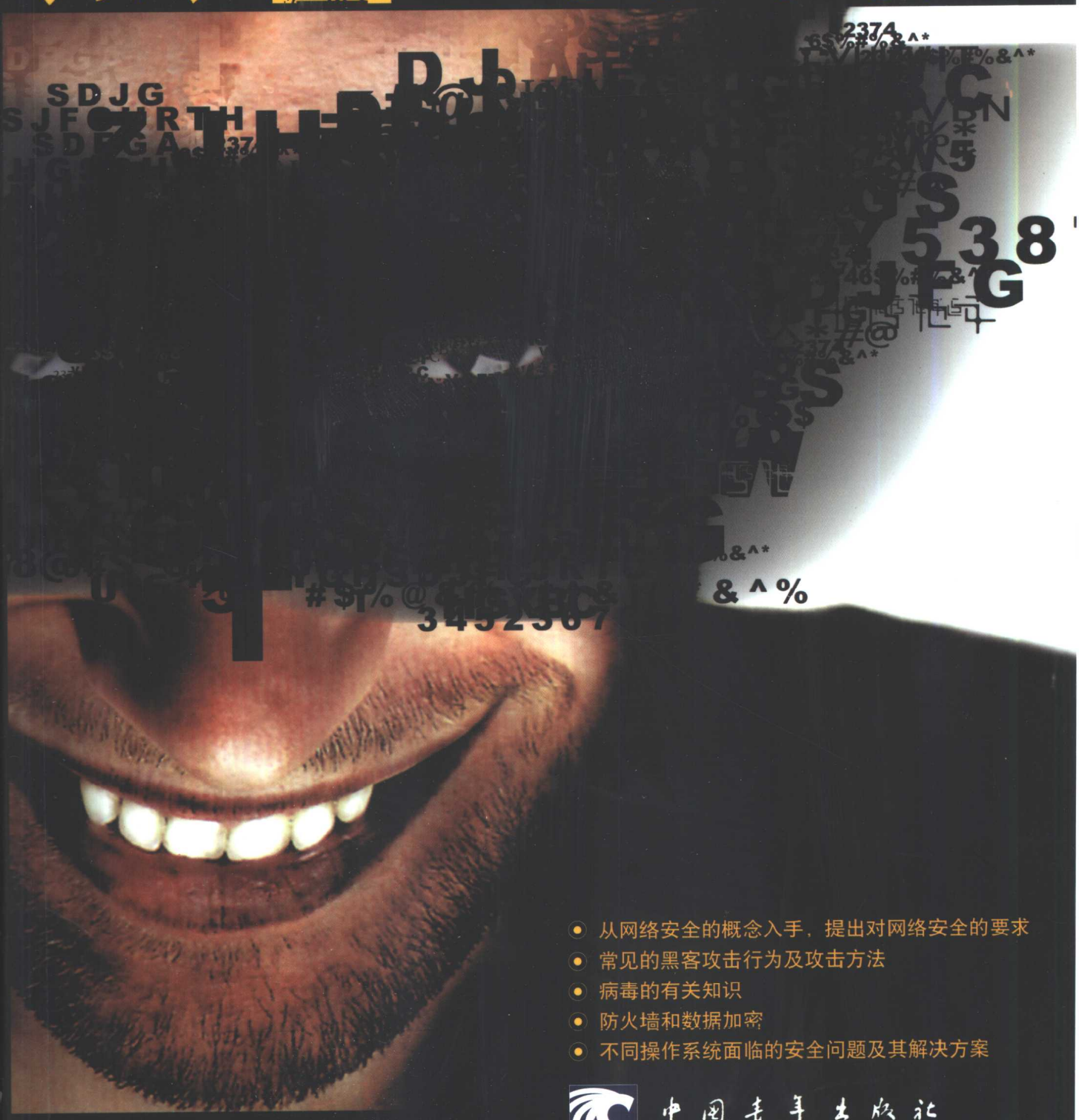
玉宏 / 等著

黑客与防护

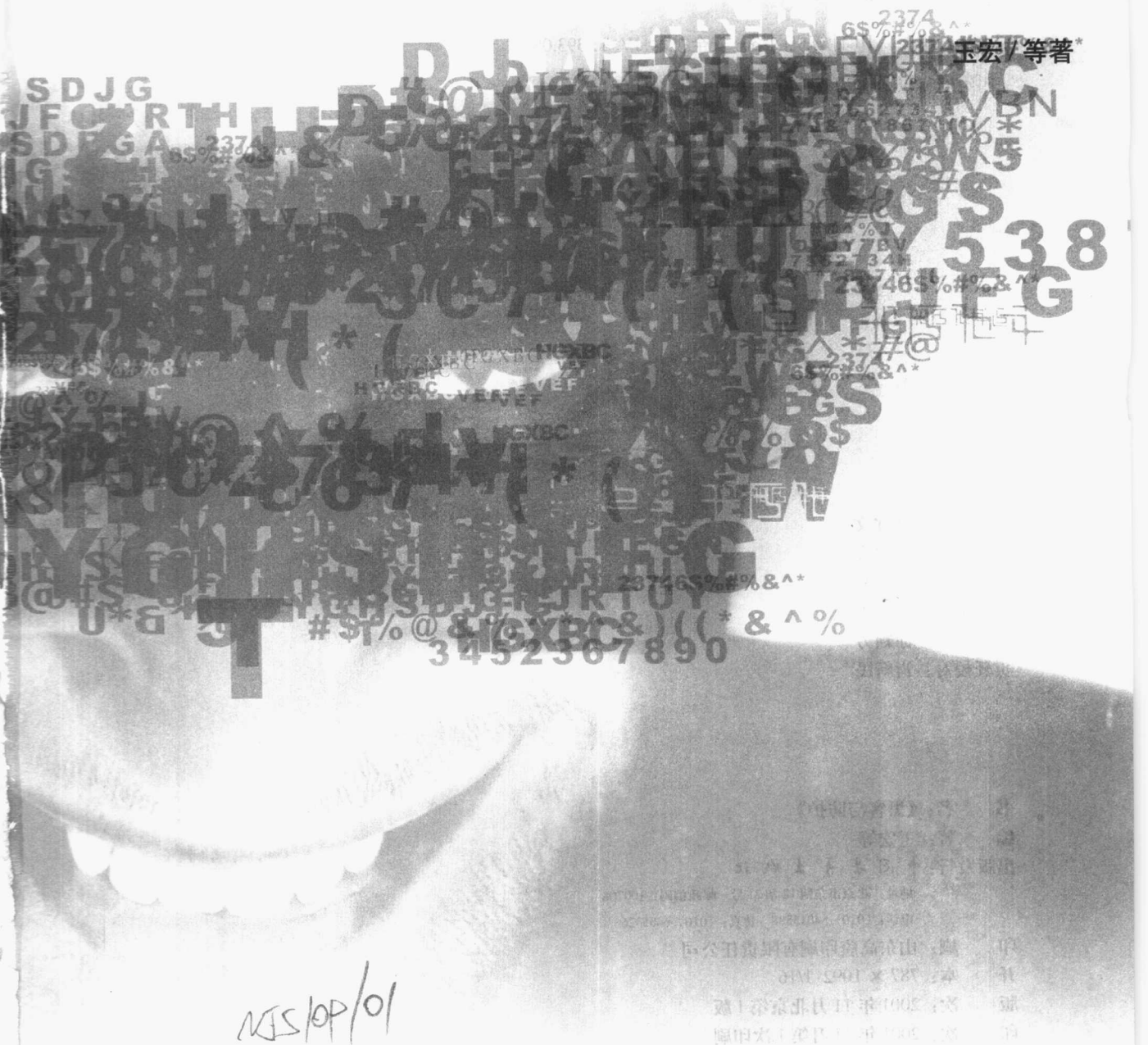


- 从网络安全的概念入手，提出对网络安全的要求
- 常见的黑客攻击行为及攻击方法
- 病毒的有关知识
- 防火墙和数据加密
- 不同操作系统面临的安全问题及其解决方案

中国青年出版社

黑客与防护

王宏广等著



中国青年出版社
CHINA YOUTH PRESS

（京）新登字 083 号

图书在版编目(CIP)数据

黑客与防护 / 玉宏等著. —北京：中国青年出版社，2001
ISBN 7-5006-4569-4

I. 黑... II. 玉... 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(2001)第 065669 号

策　　划：胡守文
　　王修文
　　郭　光
责任编辑：江　颖
　　涂颖芳
责任校对：肖新民

书　　名：《黑客与防护》
编　　著：玉宏等
出版发行：中国青年出版社
　　地址：北京市东四 12 条 21 号　邮政编码：100708
　　电话：(010) 84015588　传真：(010) 64053266
印　　刷：山东高唐印刷有限责任公司
开　　本：787 × 1092　1/16
版　　次：2001 年 11 月北京第 1 版
印　　次：2001 年 11 月第 1 次印刷
印　　数：1-5000
书　　号：ISBN 7-5006-4569-4/TP · 222
定　　价：29.00 元

前　言

很高兴能和大家在这本书里一起讨论网络方面的问题。我们和你一样，作为一个网络的忠实的爱好者，对于网络问题有着浓厚的兴趣，同时也为网络中出现的种种安全问题感到不安。所以我们写了这本书，和大家一起来探讨网络安全问题。

网络给人们带来了很大的方便，网络使人们能够足不出户就获得大量的最新信息，使人们能够坐在办公室里就能进行所有以前必须面对面的商业活动，如此等等。网络确实给人们带来了极大的方便，它的出现使地球一下子小了很多，这些都是大家有目共睹的。然而你是否意识到，在这些好处的后面却有可能潜伏着致命的陷阱，国家机密泄露、金融系统入侵、企业商机泄露、个人隐私被窃取、网络瘫痪、病毒发作等等这些令人们头疼不已的网络安全问题统统冒了出来，当然这些问题也随时可能对你造成危害。

如今网络信息安全已成为世界性的现实问题，信息安全与国家安全、民族兴衰和战争胜负息息相关，它已成为了国家和民族的头等大事，这已经被血的教训所证明。没有信息安全，就没有完全意义上的国家安全，也没有真正的政治安全、军事安全和经济安全。对于市场上激烈竞争的企业来说，问题也是同样严重，随着网上经济活动的增多，网络信息安全对于企业的正常经营也是生死攸关的。而对于个人来说，网络安全问题的存在意味着我们的个人隐私权将得不到保证。所以，面对日益明显的经济、信息全球化趋势，我们既要看到网络经济带给我们的发展机遇，也要正视它带来的严峻挑战。

面向数据的安全概念是数据的保密性、完整性和可获性，而面向使用者的安全概念则是鉴别、授权、访问控制、抗否认性和可服务性以及基于内容的个人隐私、知识产权等的保护。这两者结合就是信息安全体系结构中的安全服务，而这些安全问题又要依靠密码、数字签名、身份验证技术、防火墙、安全审计、灾难恢复、病毒防护、防黑客入侵等安全机制（措施）加以解决。其中密码技术和管理是信息安全的核心，安全标准和系统评估是信息安全的基础。总之，从历史的人网大系统的概念出发，现代的信息安全涉及个人权益、企业生存、金融风险防范、社会稳定和国家的安全。所以说网络信息安全是物理安全、网络安全、数据安全、信息内容安全、信息基础设施安全与公共信息安全的总和。

本书从介绍网络安全的概念入手，第一章介绍了网络安全的基本概念和基础知识，对网络安全性要求做了综述，介绍了一些基本的安全问题，如网络本身的问题，恶意攻击。第二章介绍了黑客技术，着重写了黑客的攻击行为和攻击方法。第三章介绍了病毒的有关知识，包括病毒的特征、病毒的原理、常见病毒实例及杀毒方法。第四章详细介绍了防火墙的原理，具体介绍了实用防火墙的安装、工作方式及安全的实现过程。第五章介绍数据加密技术，本章介绍了数据加密的作用、历史和原理和流行的加密技术，让读者能对数据加密有一个全面的了解。第六章介绍操作系统的安全，本章中介绍了不同的操作系统所面临的各自的安全问

题及其解决的方案。

希望通过对本书的阅读，你能有所收获，这就是我们三位作者最大的满足。由于作者水平和时间有限，不足之处在所难免，恳请各位批评指正。

作　者

2001 年 5 月于北京

目 录

第1章　网络安全概述

本章主要介绍网络安全的内容、安全的要求、标准以及网络安全所面临的各种威胁和解决这些问题的办法。相信通过本章的阅读，你可以对网络安全有大致的了解。

1.1　网络信息安全与保密

网络信息安全与保密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。因此网络的安全对于网络开发和管理人员来说无疑是非常重要的。

1.1.1　网络信息安全与保密的内涵

从技术角度看，网络信息安全与保密是一个涉及计算机技术、网络技术、通信技术、密码技术、信息安全、应用数学、数论、信息论等多种学科的边缘性综合学科。网络信息安全与保密的重要性有目共睹。特别是随着全球信息基础设施和各国信息基础设施的逐渐形成，国与国之间变得“近在咫尺”。网络化、信息化已成为现代社会的一个重要特征。网络信息本身就是时间，就是财富，就是生命，就是生产力。实际上，网络的快速普及已使客户端软件多媒体化、协同计算、资源共享、开放、远程管理化，电子商务、金融电子化等成为网络时代必不可少的产物。

事物总是辨证统一的。科技进步在造福人类的同时，也带来了新的危害。从某种意义上讲，网络信息系统的广泛普及，就象一个打开了的潘多拉魔盒，使得新的邪恶与罪孽相伴而来。网络信息系统中的各种犯罪活动已经严重地危害着社会的发展和国家的安全，也给人们带来了许多新的课题。网络信息安全与保密便是这些众多新课题中最具代表性的例子。

1.1.2　网络信息安全与保密的特征

通常网络信息安全与保密主要是指保护网络信息系统，使其在没有危险、不受威胁、不出事故的安全环境中运行。从技术角度来说，网络信息安全与保密的技术特征主要表现在系统的可靠性、可用性、保密性、完整性、不可抵赖性、可控性等几个方面。下面我们就这些方面一一进行介绍。

1. 可靠性

可靠性是网络信息系统能够在规定条件下和规定的时间内完成规定的功能的特性。可靠性是系统安全的最基本的要求之一，是所有网络信息系统建设和运行的目标。

网络信息系统的可靠性测度主要有三种：抗毁性、生存性和有效性。

抗毁性是指系统在人为破坏下的可靠性。比如，部分线路或节点失效后，系统是否仍然能够提供一定程度的服务。增强抗毁性可以有效地避免因各种灾害（战争、地震等）造成的

大面积瘫痪事件。

生存性是指在随机破坏下系统的可靠性。生存性主要反映随机性破坏和网络拓扑结构对系统可靠性的影响。这里，随机性破坏是指系统部件因为自然老化等造成的自然失效。

有效性是一种基于业务性能的可靠性。有效性主要反映在网络信息系统的部件失效情况下，系统满足业务性能要求的程度。比如，网络部件失效虽然没有引起连接性故障，但是却造成质量指标下降、平均延时增加、线路阻塞等现象。

可靠性主要表现在硬件可靠性、软件可靠性、人员可靠性、环境可靠性等方面。硬件可靠性最为直观和常见。软件可靠性是指在规定的时间内，程序成功运行的概率。人员可靠性是指人员成功地完成工作或任务的概率。人员可靠性在整个系统可靠性中扮演重要角色，因为系统失效的大部分原因是人为差错造成的。人的行为要受到生理和心理的影响，受到其技术熟练程度、责任心和品德等素质方面的影响。因此，对人员的教育、培养、训练和管理以及合理的人机界面是提高可靠性的重要方法。环境可靠性是指在规定的环境内，保证网络成功运行的概率。这里的环境主要是指自然环境和电磁环境。

2. 可用性

可用性是网络信息可被授权实体访问并按需求使用的特性，即网络信息服务在需要时，允许授权用户或实体使用的特性；或者是网络部分受损或需要降级使用时，仍能为授权用户提供有效服务的特性。可用性是网络信息系统面向用户的安全性能。网络信息系统最基本的功能是向用户提供服务，而用户的需求是随机的、多方面的，有时还有时间要求。可用性一般用系统正常使用时间和整个工作时间之比来度量。

可用性还应该满足以下要求：身份识别与确认、访问控制（对用户的权限进行控制，只能访问相应权限的资源，防止或限制经隐蔽通道的非法访问。包括自主访问控制和强制访问控制）、业务流控制（利用均分负荷方法，防止业务流量过度集中而引起网络阻塞）、路由选择控制（选择那些稳定可靠的子网，中继线或链路等）、审计跟踪（把网络信息系统中发生的所有安全事件情况存储在安全审计跟踪之中，以便分析事故原因，分清责任，及时采取相应的措施。审计跟踪的信息主要包括：事件类型、被管客体等级、事件时间、事件信息、事件回答以及事件统计等方面的信息）。

3. 保密性

保密性是网络信息不被泄露给非授权的用户、实体或过程，或供其利用的特性。即防止信息泄漏给非授权个人或实体，信息只为授权用户使用的特性。保密性是在可靠性和可用性基础之上，保障网络信息安全的重要手段。

常用的保密技术包括以下几个方面：防侦收（使对手侦收不到有用的信息）、防辐射（防止有用信息以各种途径辐射出去）、信息加密（在密钥的控制下，用加密算法对信息进行加密处理。即使对手得到了加密后的信息也会因为没有密钥而无法读懂有效信息）、物理保密（利用各种物理方法，如限制、隔离、掩蔽、控制等措施，保护信息不被泄露）。

4. 完整性

完整性是网络信息在未经授权的情况下不能被进行改变的特性。即网络信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏和丢失的特性。完整性是一种面向信息的安全性，它要求保持信息的原样，即信息的正确生成和正确存储及传输。

完整性与保密性不同，保密性的目的是要求信息不被泄露给未授权的人，而完整性的目的则是要求信息不致受到各种原因的破坏。影响网络信息完整性的主要因素有以下几种：设备故障、误码（包括传输、处理和存储过程中产生的误码，定时的稳定度和精度降低造成的误码，各种干扰源造成的误码等）、人为攻击、计算机病毒等。

保障网络信息完整性的主要方法有：

（1）协议：通过各种安全协议可以有效地检测出被复制的信息、被删除的字段、失效的字段和被修改的字段；

（2）纠错编码方法：由此完成检错和纠错功能。最简单和常用的纠错编码方法是奇偶校验法；

（3）密码校验和方法：它是抗窜改和传输失败的重要手段；

（4）数字签名：保障信息的真实性；

（5）公证：请求网络管理或中介机构证明信息的真实性。

5. 不可抵赖性

不可抵赖性也称作不可否认性，在网络信息系统的信息交互过程中，确信参与者的真实同一性。即所有参与者都不可能否认或抵赖曾经完成的操作和承诺。利用信息源证据可以防止发信方不真实地否认已发送信息，利用递交接收证据可以防止收信方事后否认已经接收的信息。

6. 可控性

可控性是对网络信息的传播及内容具有控制能力的特性。概括地说，网络信息安全与保密的核心是通过计算机、网络、密码技术和安全技术，保护在公用网络信息系统中传输、交换和存储的消息的保密性、完整性、真实性、可靠性、可用性、不可抵赖性等。

网络信息安全与保密的不同含义：与其他概念不同的是，网络信息安全与保密的具体含义和侧重点会随着观察者的角度而不断变化，比如：

从用户（个人用户或者企业用户）的角度来说，他们最为关心的网络信息安全与保密问题是如何保证他们的涉及个人隐私或商业利益的数据在传输过程中受到保密性、完整性和真实性的保护。避免其他人（特别是其竞争对手）利用窃听、冒充、篡改、抵赖等手段对其利益和隐私造成损害和侵犯，同时用户也希望他保存在某个网络信息系统中的数据，不会受到其他非授权用户的访问和破坏。

从网络运行和管理者角度说，他们最为关心的网络信息安全与保密问题是如何保护和控制其他人对本地网络信息的访问、读写等操作。比如，避免出现“陷门”、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现象，制止和防御网络“黑客”的攻击。

对安全保密部门和国家行政部门来说，他们最为关心的网络信息安全与保密问题是如何对非法的、有害的或涉及国家机密的信息进行有效过滤和防堵，避免非法泄露。机密敏感的信息被泄密后将会对社会的安定产生危害，对国家造成巨大的经济损失和政治损失。

从社会教育和意识形态角度来说，他们最为关心的网络信息安全与保密问题是如何杜绝和控制网络上不健康的内容。有害的黄色内容会对社会的稳定和人类的发展造成不良影响。

1.1.3 网络信息安全与保密的层次结构

网络信息安全与保密的层次结构主要包括：物理安全、安全控制和安全服务。

1. 物理安全

物理安全是指在物理介质层次上对存贮和传输的网络信息的安全保护。物理安全是网络信息安全的最基本保障，是整个安全系统不可缺少和忽视的组成部分。一方面，在各种软件和硬件系统中要充分考虑到系统所受的物理安全威胁和相应的防护措施；另一方面，也要通过安全意识的提高、安全制度的完善、完全操作的提倡等方式使用户和管理维护人员在物理层次上实现对网络信息的有效保护。目前，该层次上常见的不安全因素包括三大类：

（1）自然灾害（如地震、火灾、洪水等）、物理损坏（如硬盘损坏、设备使用寿命到期、外力破损等）、设备故障（如停电断电、电磁干扰等）。此类不安全因素的特点是：突发性、自然性、非针对性。这种不安全因素对网络信息的完整性和可用性威胁最大，而对网络信息的保密性影响却较小，因为在一般情况下，物理上的破坏将销毁网络信息本身。解决此类不安全隐患的有效方法是采取各种防护措施、制定安全保护规章制度、随时进行数据备份等。

（2）电磁辐射（如侦听微机操作过程）、乘机而入（如合法用户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，被非法用户获得）等。此类不安全因素的特点是：隐蔽性、人为实施的故意性、信息的无意泄露性。这种不安全因素主要破坏网络信息的保密性而对网络信息的完整性和可用性影响不大。解决此类不安全隐患的有效方法是采取辐射防护、屏幕口令、隐藏销毁等。

（3）操作失误（如偶然删除文件、格式化硬盘、线路拆除等）、意外疏漏（如系统掉电、“死机”等系统崩溃）。此类不安全因素的特点是：人为实施的无意性和非针对性。这种不安全因素主要破坏网络信息的完整性和可用性，而对保密性影响不大。解决此类不安全隐患的有效方法是：状态检测、报警确认、应急恢复等。

2. 安全控制

安全控制是指在网络信息系统中对存贮和传输的信息的操作和进程进行控制和管理，重点是在网络信息处理层次上对信息进行初步的安全保护。安全控制可以分为以下三个层次：

（1）操作系统的安全控制。包括：对用户的合法身份进行核实（如开机时要求键入口令）、对文件的读写存取的控制（如文件属性控制机制）。此类安全控制主要保护被存贮数据的安全。

（2）网络接口模块的安全控制。在网络环境下对来自其他机器的网络通信进程进行安

全控制。此类控制主要包括身份认证、客户权限设置与判别、审计日志等。

（3）网络互联设备的安全控制。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监测和控制。此类控制主要通过网管软件或路由器配置实现。需要指明的是，安全控制主要通过现有的操作系统或网管软件、路由器配置等实现。安全控制只提供了初步的安全功能和网络信息保护。

3. 安全服务

安全服务是指在应用程序层对网络信息的保密性、完整性和信源的真实性进行保护和鉴别，满足用户全需求，防止和抵御各种安全威胁和攻击手段。安全服务可以在一定程度上弥补和完善现有操作系统和网络信息系统的安全漏洞。安全服务的主要内容包括：安全机制、安全连接、安全协议、安全策略等。

（1）安全机制是利用密码算法对重要而敏感的数据进行处理。比如，以保护网络信息的保密性为目标的数据加密和解密；以保证网络信息来源的真实性和合法性为目标的数字签名和签名验证；以保护网络信息的完整性，防止和检测数据被修改、插入、删除和改变为目标的信息认证等。安全机制是安全服务乃至整个网络信息安全系统的核心和关键。现代密码学在安全机制的设计中扮演着重要的角色。

（2）安全连接是在安全处理前与网络通信方之间的连接过程。安全连接为安全处理进行了必要的准备工作。安全连接主要包括会话密钥的分配和生成和身份验证。后者旨在保护信息处理和操作的对等双方的身份真实性和合法性。

（3）安全协议。协议是多个使用方为完成某些任务所采取的一系列的有序步骤。协议的特性是：预先建立、相互同意、非二义性和完整性。安全协议使网络环境下互不信任的通信方能够相互配合，并通过安全连接和安全机制的实现来保证通信过程的安全性、可靠性和公平性。

（4）安全策略。安全策略是安全机制、安全连接和安全协议的有机组合方式，是网络信息系统安全性的完整的解决方案。安全策略决定了网络信息安全系统的整体安全性和实用性。不同的网络信息系统和不同的应用环境需要不同的安全策略。

1.1.4 网络信息安全与保密的环境变迁

网络信息安全与保密的含义还会因为不同的应用环境得到不同的解释。大体上可以分为：

（1）运行系统安全：即保证网络信息处理和传输系统的安全。包括计算机系统机房环境的保护，法律、政策的保护，硬件系统的可靠运行，操作系统的安全，电磁信息泄露的防护等。安全的运行系统侧重于保证网络信息系统的正常运行。避免因为系统崩溃和损坏而对存贮、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，或被他人干扰。运行系统安全的本质是保护系统的合法操作和正常运行；

（2）网络系统信息的安全：如用户口令鉴别、用户存取权限控制、数据存取权限和方式控制、安全审计、安全跟踪、计算机病毒防治、数据加密等；

（3）网络信息传播的安全：即网络信息传播后果的安全。比如，对不良网络信息进行有效过滤。网络信息传播的安全侧重于防止和控制非法、有害的信息传播。避免公用网络信息系统中大量自由传输的数据失控。网络信息传播安全的本质是维护社会道德、国家法规和人民利益；

（4）网络信息内容的安全：它侧重于保护信息的保密性、真实性和完整性。避免攻击者利用网络信息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。网络信息内容安全的本质是保护用户的利益和隐私。

由此可见，网络信息安全与保密是一个很复杂的问题，它与被保护的对象密切相关。还有一种观点认为，网络信息安全与保密包括以下几个方面：物理安全、人员安全、符合瞬时电磁脉冲辐射标准、信息安全、操作安全、通信安全、计算机安全、工业安全等。网络信息安全与保密的本质是在安全期内保证数据在网络上传输或存贮时不被非授权用户非法访问，但授权用户却可以访问。

1.2 网络攻击

网络往往会在运行过程中受到各种各样的攻击，网络信息的安全与保密所面临的威胁来自很多方面，并且随着时间的变化而变化。这些威胁可以宏观地分为人为威胁和自然威胁。

自然威胁可能来自于各种自然灾害、恶劣的场地环境、电磁辐射和电磁干扰、网络设备自然老化等。这些无目的的事件，有时会直接威胁网络信息安全，影响信息的存储媒体。

这里重点讨论人为威胁。此种威胁，通过攻击系统暴露的要害或弱点，使得网络信息的保密性、完整性、可靠性、可控性、可用性等受到伤害。人为威胁又分为两种：一种是以操作失误为代表的无意威胁（偶然事故），虽然人为的偶然事故没有明显的恶意企图和目的，但它会使信息受到严重破坏。最常见的偶然事故有：操作失误（未经允许使用、操作不当、误用存储媒体等）、意外损失（电力线路搭接、漏电、电焊火花干扰）、编程缺陷（经验不足、检查漏项、水平所限）、意外丢失（被盗、被非法复制、丢失媒体）、管理不善（维护不力、管理薄弱、纪律松懈）、无意破坏（犁地割线）。另一种是以计算机犯罪为代表的有意威胁（恶意攻击）。要防范这些攻击，我们就要先了解这些攻击的类型和各自的特点，从而寻找到保护网络安全的方法，下面就这些攻击类型做详细的介绍。

1.2.1 恶意攻击

恶意攻击是人为的有目的的对网络的攻击。恶意攻击可以分为主动攻击和被动攻击。主动攻击是指以各种方式有选择地破坏信息（如：修改、删除、伪造、添加、重放、乱序、冒充等）。被动攻击是指在不干扰网络信息系统正常工作的情况下，进行侦收、截获、窃取、破译信息等。

由于人为恶意攻击主要来自有明显企图的攻击者，其危害性相当大，给国家安全、知识产权和个人信息带来巨大的威胁。人为恶意攻击具有以下特性：

（1）智能性：从事恶意攻击的人员大都具有相当高的专业技术和熟练的操作技能。他们的文化程度高，许多人都是具有一定社会地位的部门业务主管。他们在攻击前都经过了周密的预谋和精心策划。

（2）严重性：涉及到金融资产的网络信息系统恶意攻击，往往会由于资金损失巨大，而使金融机构、企业蒙受重大损失，甚至破产，同时，也给社会稳定带来震荡。如美国资产融资公司计算机欺诈案，涉及金额 20 亿美元之巨，犯罪影响震荡全美。在我国也发生数起计算机盗窃案，金额在数万到数百万人民币，给国家金融资产带来严重损失。

（3）隐蔽性：人为恶意攻击的隐蔽性很强，不易引起怀疑，作案的技术难度大。一般情况下，其犯罪的证据，存在于软件的数据和信息资料之中，若无专业知识很难获取侦破证据。相反，犯罪行为人却可以很容易地毁灭证据，计算机犯罪的现场也不象是传统犯罪现场那样明显。

（4）多样性：随着计算机互联网的迅速发展，网络信息系统中的恶意攻击也随之发展变化。出于经济利益的巨大诱惑，近年来，各种恶意攻击主要集中于电子商务和电子金融领域。攻击手段日新月异，新的攻击目标包括偷税漏税、利用自动结算系统洗钱以及在网络上进行盈利性的商业间谍活动等等。

国际互联网上以人为恶意攻击为代表的高技术犯罪的另一大发展趋势是网络犯罪集团化。现在黑客已经不再单兵作战了，他们有自己的地下组织、自己的站点，如果一个缺陷被发现，很快就会在黑客间传开。由于网络上的安全机制不断加强，今后的网络犯罪将需要比今天高得多的技术力量，这种客观要求加上网络上日益增长的经济利益将诱使计算机犯罪集团尤其是跨国犯罪集团将黑手伸向网络信息系统。因此，传统犯罪活动和网络犯罪的融合将对各国司法当局和国际反犯罪机构提出更大的挑战。

网络犯罪现在已经成为犯罪学研究领域的一部分，这些罪犯知识水平高、危害性大，而且隐蔽性很强。现在，在因特网上实行商业、银行抢劫的越来越多，黑客不单是一些想显示自己计算机水平的好奇的大学生，更有一些专职的商业间谍。在美国，许多银行开始连入因特网，用户可以在因特网上存取银行里的钱，纽约的道琼斯股票交易所也提供了自动控制网服务，股民可以在网上买卖股票，而这些服务对黑客来说确实具有诱惑力。除了对钱财的贪婪，还有一些黑客的入侵是出于其他目的。例如，最近，有人在网上听说印尼一家报纸的 WWW 服务器被一个中国黑客入侵了，据说是出于对印尼政府的不满。因为在 1998 年 5 月印尼发生的暴乱中，许多印尼华侨被抢劫、杀戮、强奸，而印尼政府并没有采取有效的措施来解决这个问题。

另一种对公司危害极大的入侵是被解雇的职员出于对公司的不满而入侵内部网络，这种入侵危害大是因为入侵者对内部网络很了解，所以往往会造成比较致命的破坏。因此，网络管理员及时删去离职人员的帐户是很重要的，当然，因个人水平不同、攻击目的不同，黑客对网络实施入侵的水平也大不相同。

一般来说，最低层的入侵就是电子邮件炸弹，这种入侵纯粹是出于报复，这种网络危害不算很大，只可能会造成拒绝服务；再深一层的入侵就是得到了一些不该有的权限，如偷看

别人的邮件或获得了有限的非法的写权力；最高的一层是入侵者得到了 root 权限，对网络可以进行任意地破坏，而报导的有些高级入侵者本身就是一些大机构的系统管理员或安全顾问。1994 年，美国一家大机构的安全顾问被逮捕了，他是一个很有影响力的系统管理员，他也曾在 BELL 实验室工作过，但他却多次入侵了 Intel 公司，直到他被一个网络管理员发现。

下面简要介绍一些有代表性的恶意攻击：

（1）窃听：为什么网络易被窃听和欺骗？

首先论述为什么网络极易被窃听，这需要从局域网的特点说起，因特网是一种网间网技术，其实它就是把无数的局域网相连起来形成大的网，然后再把大的网连成更大的网。因特网的拓扑是一种逐步细化的树状结构，虽然因特网上的传输是点对点的，但一般因特网上的主机会处于一个局域网中，例如清华开放实验室是一个局域网，它连到了校园网，又连到了中国教育科研网（CERNET），中国教育科研网又连接到国外。局域网，如以太网、令牌网，都是广播型网络，也就是说一台主机发布消息，网上任何一台机器都可以收到这个消息，每个节点都能读取网上的数据。对广播网络的基带同轴电缆或双绞线进行搭线窃听是很容易的，安装通信监视器和读取网上的信息也很容易。网络体系结构允许监视器接收网上传输的所有数据帧而不考虑帧的传输目的地址，这种特性使得偷听网上的数据或非授权访问很容易且不易被发现。一般情况下，以太网卡在收到发往别人的消息时会自动丢弃消息，而不向上层传递消息。但以太网卡的接收模式可以设置成混合型（promiscuous），这样网卡就会捕捉所有的数据包，并把这些数据包向上传递，这就是为什么以太网可以被窃听，其实 FDDI、令牌网也存在这样的问题。现在人们经常谈论的 ATM 网络技术是点对点的，它不会像以太网的广播式那样容易被窃听。

因特网上的信息，容易被窃听和截获的另一个原因是，当某人用一台主机和国外的主机进行通信时，他们之间互相发送的数据包是经过很多机器重重转发的。例如，用户在清华开放实验室的一台主机上访问 Hotmail 主机，用户的数据包要经过开放实验室的路由器，清华校园路由器，中国教育科研网上的路由器，然后从中国教育科研网的总出口出国，再经过很多网络和路由器才能到达 Hotmail 主机。具体要经过多少主机、多少路由器和多少网络，用户可以用一个网络调试工具得到，这个工具就是 Traceroute，在各种操作系统中都有，如 Windows95、Windows NT 和 UNIX，名字上可能会有所差异，但功能和实现上是一样的。

因特网的这种工作原理不仅节约了资源，而且简化了传输过程的实现，符合 TCP/IP 简单高效的宗旨，但这也带来了安全上的问题。当然，用户不可能力求安全而放弃这种方法，因为这样做是不实际的，也是不必要的。用户所能做到的只是意识到这种问题，并以其他办法来提高安全性，如在第五章所讲的加密的方法。

再回到安全这个画龙点睛题上来，试想黑客可以使用一台处于用户的数据包传输路径上的主机，那么他就可以窃听或劫持用户的数据包。例如，处于中国教育科研出口的一台机器可以监听所有从这个网络出国的数据包。每当谈到网络窃听，大家总是想到有人用厂里的总机窃听别人电话的谈话内容。当时，厂里所有的电话都要经过厂里总机，可总机并不是程控的，而是人工接线的，所以接线员极易窃听别人的电话，这就有些类似刚才讲的网络窃听。

网络窃听可能是出于好奇，也可能是出于恶意的。现在越来越多的黑客不再是喜欢破坏公物的人，而是商业间谍，所以网络安全是把因特网真正推向商业化所必须考虑和解决的问题。

（2）信息战：这是一种以获得信息权为目标的无硝烟的战争。信息战可以说是一种国家行为的恶意攻击。信息战的攻击目标包括各种军事命令、通信系统、能源、运输和金融等与国家的政治、经济、文化密切相关的系统。在和平时期，信息战处于绝对隐蔽状态，但是一旦战争爆发，信息战将出其不意地发挥出巨大的破坏力。美军在伊拉克实施的“沙漠风暴”战争便是典型的信息战例。

（3）商业间谍：利用国际互联网收集别国的重要商业情报，其目标是获得有价值的信息、能力、技术和对自身有利的谈判地位。在多数情况下，商业间谍属于一种集团行为的恶意攻击。

除了以信息战为代表的国家行为恶意攻击和以商业间谍为代表的集团行为恶意攻击之外，还有众多的个人行为或者小团体行为的恶意攻击，此类恶意攻击数量巨大，目的复杂。有的恶意攻击者来自窃贼、骗子、敲诈、毒犯、犯罪组织成员和其他有犯罪行为的人。有的恶意攻击者来自黑客、恶意竞争者、心怀不满的工作人员、个人仇敌等。此类恶意攻击的手段有：

（4）流量分析：它能通过对网上信息流的观察和分析推断出网上的数据信息，比如有无传输、传输的数量、方向、频率等。因为网络上的所有节点都能访问全网，所以流量的分析易于完成。由于报头信息不能被加密，所以即使对数据进行了加密处理，也可以进行有效的流量分析。

（5）破坏完整性：有意或无意地修改或破坏信息系统，或者在非授权和不能监测的方式下对数据进行修改。

（6）重发：重发是重复一份报文或报文的一部分，以便产生一个被授权效果。当节点拷贝发到其他节点的报文并在其后重发他们时，如果不能监测重发，节点依据此报文的内容接受某些操作，例如报文的内容是关闭网络的命令，则将会出现严重的后果。

（7）假冒：当一个实体假扮成另一个实体时，就发生了假冒。一个非授权节点，或一个不被信任的、有危险的授权节点都能冒充一个授权节点，而且不会有多大困难。很多网络适配器都允许网帧的源地址由节点自己来选取或改变，这就使冒充变得较为容易。

（8）拒绝服务：当一个授权实体不能获得对网络资源的访问或当紧急操作被推迟时，就发生了拒绝服务。拒绝服务可能由网络部件的物理损坏而引起，也可能由使用不正确的网络协议而引起（如传输了错误的信号或在不适当的时候发出了信号），或者是由超载而引起。

（9）资源的非授权使用：即与所定义的安全策略不一致的使用。因常规技术不能限制节点收发信息，也不能限制节点侦听数据，一个合法节点能访问网络上的所有数据和资源。

（10）干扰：干扰是由一个节点产生数据来扰乱提供给其他节点的服务。干扰也能由一个已经损坏的并还在继续传送报文的节点所引起，或由一个已经被故意改变成具有此效果的节点所引起。频繁的令人讨厌的电子邮件信息是最典型的干扰形式之一。

（11）病毒：目前，全世界已经发现了上万种计算机病毒。它们的类型及数量大体为：DOS 型 10000～11000 种、Windows 型 12 种、UNIX 型 6 种、宏病毒 200 余种、Macitoch 型 35 种、和众多的 E-mail 病毒。计算机病毒的数量已有了相当的规模，并且新的病毒还在不断出现。比如，最近保加利亚计算机专家迈克·埃文杰制造出了一种计算机病毒“变换器”，它可以设计出新的更难发现的“多变形”病毒。该病毒具有类似神经网络细胞式的自我变异功能，在一定的条件下，病毒程序可以无限制的衍生出各种各样的变种病毒。随着计算机技术的不断发展和人们对计算机系统和网络依赖程度的增加，计算机病毒已经构成了对计算机系统和网络的严重威胁。这些病毒可以随下载的软件，如 Java 程序、ActireX 控件进入公司的内部网络。病毒程序中有一种被称为特洛伊木马的程序，这种程序表面上是无害的，具有很强的隐蔽性，但实际上在背后破坏用户的网络。虽然现在有些防火墙声称具有强大的功能，但新的病毒、旧病毒的变异品种仍会溜进用户的网络。

（12）诽谤：利用网络信息系统的广泛互联性和匿名性，散布错误的消息以达到诋毁某人或某公司形象和知名度的目的。

1.2.2 防不胜防的黑客

在现实生活中，通过密码攻击计算机网络系统的事件时有发生，这些攻击者想方设法侵入系统，给网络安全带来了无尽的忧虑，这些未经允许而非法进入的攻击者常被人们称为“黑客”。

1. 黑客的行为特征

什么样的人可以被称为“黑客”呢？

世界各地对黑客的“定义”都不尽相同。按照东方人的习惯通常对黑客一词还有“侠”的含意。日本 1998 年新出版的《新黑客字典》把黑客定义为：“喜欢探索软件程序奥秘、并从中增长其个人才干的人。他们不像绝大多数电脑使用者，只规规矩矩地了解别人指定了解的狭小部分知识。”1998 年夏季，印尼华人妇女惨遭印尼暴徒有组织的强暴，被激怒的中国黑客奋起袭击并破坏印尼诸站点的事例，则是一种典型的侠客行为。现在“黑客”一词在信息安全范畴内的普遍含意是特指对电脑系统的非法侵入者。多数黑客对电脑非常着迷，认为自己是世界上绝顶聪明的人，能够成为他人所不为或不能为的人。只要他们愿意，就可肆无忌惮非法闯入某些敏感数据的禁区或是内部网络，盗取重要的信息资源，或是与某些政府要员甚至是总统开一个玩笑，或者干脆针对某些人进行人身攻击、诽谤或恶作剧。他们常常以此为乐，将其作为一种智力的挑战而陶醉。国际上的著名黑客大多是 15-30 岁的年轻人，他们有着共同的伦理观：信息、技术和诀窍都应当被所有用户共享，而不能为个别人或集团所垄断。这些人在计算机方面的天赋，使其常常处于高度兴奋状态，他们会彻夜不眠地操纵计算机，攻破网络或信息禁区，偷看敏感数据，篡改网址信息或者删除该网址的全部内容，其行为已经造成恶劣影响。黑客中的很多人具有反社会行为或反传统文化的色彩，与西方社会的“朋客”极其相似，有的还自称为“电脑朋客”（Cyberpunks）。目前黑客已成为一个广泛的社会群体。