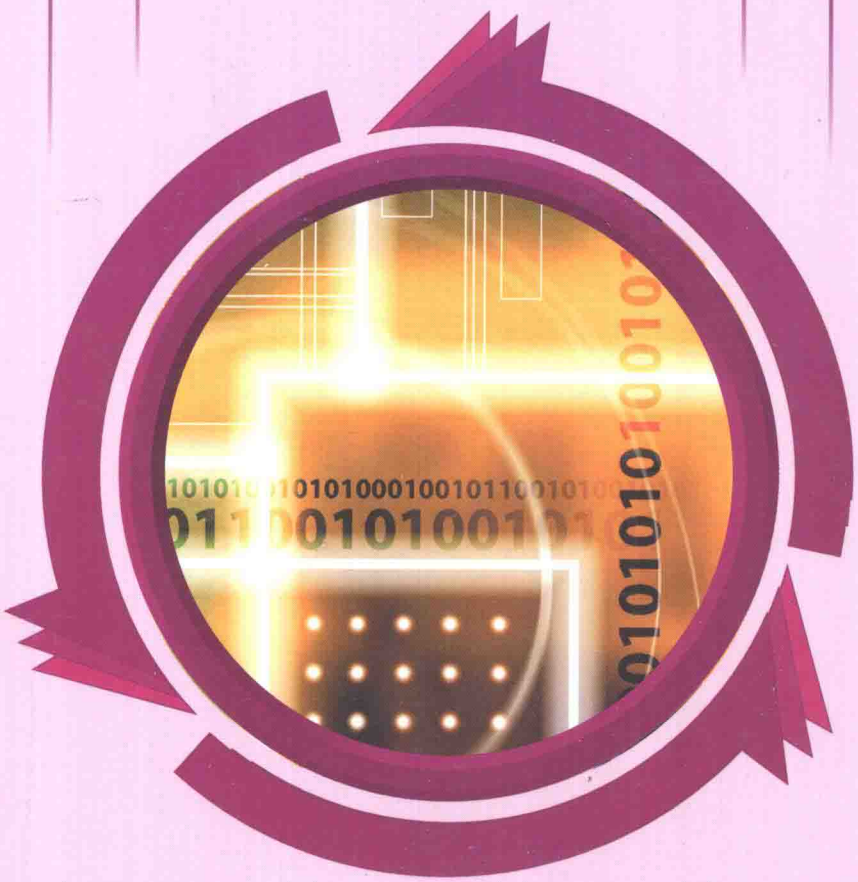
现代通信高技术丛书

智能信息安全

景晓军 主编
孙松林 周贤伟 编著



国防工业出版社
National Defense Industry Press

现代通信高技术丛书

智能信息安全

Zhineng Xinxi Anquan

景晓军 主编

孙松林 周贤伟 编著

国防工业出版社

http://www.ndip.cn

内 容 简 介

本书全面客观地介绍了网络信息安全技术的整体概念，并详细阐述了当前流行的物理网络安全技术的基本原理和功能实现等内容。

本书共分 7 章：第 1 章介绍网络信息安全相关概念；第 2 章介绍信息安全的网络基础；第 3 章介绍密码学技术；第 4 章介绍防火墙技术；第 5 章介绍计算机病毒与反病毒技术；第 6 章介绍入侵检测技术；第 7 章介绍操作系统安全。

本书涉及的内容新颖全面，基础知识讲解清楚、描述清晰，应用性极强。该书可以作为普通高等院校通信、电子、信息等专业的本科生教材或教学参考书，也可作为电信技术人员和研究人员的培训教材。

图书在版编目(CIP)数据

智能信息安全／景晓军主编；孙松林，周贤伟编著．
北京：国防工业出版社，2006.5
（现代通信高技术丛书／周贤伟，邓忠礼，郑雪峰主编）
ISBN 7-118-04482-2

Ⅰ.智… Ⅱ.①景…②孙…③周… 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(2006)第 025779 号

※

国防工业出版社出版发行
（北京市海淀区紫竹院南路 23 号 邮政编码 100044）
腾飞胶印厂印刷
新华书店经售

*

开本 787×1092 1/16 印张 16 字数 360 千字
2006 年 5 月第 1 版第 1 次印刷 印数 1—4000 册 定价 30.00 元

（本书如有印装错误，我社负责调换）

国防书店：(010)68428422 发行邮购：(010)68414474
发行传真：(010)68411535 发行业务：(010)68472764

目　录

第1章 绪 论

21世纪是信息的时代、知识经济时代。信息成为社会发展的重要战略资源，信息技术改变着人们的生活和工作方式。信息产业成为新的经济增长点。社会的信息化已成为当今世界发展的主要潮流。同时以Internet为代表的计算机网络的迅速发展和广泛应用，引起社会和经济的深刻变革，Internet已经成为我们生活中的一个不可分割的组成部分。基于计算机网络的崭新的政务形式“电子政务”、商务形式“电子商务”和金融形式“电子金融”正在兴起，引起了政务、商务、金融领域内一场深刻的变革。对此，发展我国的电子政务、电子商务和电子金融已成为建设具有中国特色社会主义强国的不可回避的选择。然而，目前影响这些技术应用的主要障碍是网络信息安全问题。由于Internet的开放性和无政府状态，使Internet成为一个不安全的网络，这使得我们对网络安全的研究势在必行。

现在世界上每年因利用计算机网络进行犯罪所造成的直接经济损失令人惊讶。据美国ABA组织调查和专家估计，美国每年因计算机犯罪所造成的经济损失高达150亿美元。据报道，在Internet上，每天大约有4起计算机犯罪发生。计算机犯罪，作为一种更为隐蔽的犯罪手段，给社会带来了很大的危害，因此计算机网络安全问题已经成为世界各国研究的热门课题。

本书旨在介绍计算机网络安全的基础知识和应用安全技术。

1.1 互联网的发展及网络安全的重要性

Internet已遍及世界上的240多个国家和地区，为用户提供多样化的网络与信息服务。TCP/IP网络的应用已经使全球互相连接的主机和网络形成了一个全局性的系统——因特网。建立因特网的本意是在政府投资的研究机构之间建立一种通信方式，并且逐步扩展至教育机构、商业组织和政府机关。在这方面，因特网在过去的10年中已经取得了极大的进步。

目前，因特网是世界上最大的计算机网络。而且，自1988年起，因特网保持着每年翻一番的增长速度，它的规模已经超过了包括公共交换电话网(PSTN, Public Switched Telephone Network)(一个实验室微机数量远远多于电话数量，现在宿舍里可能也是人手一台微机，每个微机基本都上网)在内的所有网络的规模，而成为世界第一大网。

1.1.1 互联网发展的规模

1) 国际的发展

到1998年初，因特网上已经接入了200多万台Web服务器和3亿多台计算机(IPV4可接入40亿个主机)。因此，人们把因特网看做是信息高速公路(即美国政府提出的国家信息基础设施NII)的基础和化身。

2) 国内的发展

截止 2001 年,我国上网计算机数约 892 万台,其中专线上网计算机 141 万台,拨号上网计算机 751 万台。

我国上网用户人数约 2250 万人,其中专线上网的用户人数约为 364 万,拨号上网的用户人数约为 1543 万,同时使用专线与拨号的用户人数为 343 万,除计算机外同时使用其他设备(移动终端、信息家电等)上网的用户人数为 92 万。

CN 下注册的域名总数为 122099 个,WWW 站点数(包括 .CN、.COM、.NET、.ORG 下的网站)约 265405 个,我国国际线路的总容量为 2799M。

原来的"衣、食、住、行",应改为:"衣、食、住、行、视(电视)、网"。Internet 带来了一场网络革命。

1.1.2 网络安全的重要性

开始,人们使用的互联网都是互相信任,互相开放的。在这种互信环境下,使用互联网的人就是构建互联网的人。但随后,越来越多不同目的和行为的人加入了使用因特网的行列。在媒体上有一些不可控制的使用者,这些人的行为无法控制,就像一颗颗不定时的炸弹。同时由于网络信息流通快的特性,各种软件随处都是,有些软件可以根据系统的漏洞来发动攻击。只要有心去寻找,就可以让一个计算机能力不高的人轻松地成为破坏高手。所以每一使用者都可看做是一个个随时会爆炸的不定时炸弹。因此,因特网的运行环境并非安全。现实社会中所有的危险情况都有可能出现在因特网上。除了善意、诚实的用户外,还有企图闯入计算机系统的人。为此,因特网正经受着这些恶意的威胁。在这一环境下,因特网的开放性便成了一把双刃利剑。长期以来,尤其是从 20 世纪 90 年代开始,随着因特网商业化的发展,因特网已经成为最时髦的攻击对象,其安全漏洞的扩展速度实际上已超过了互联网发展的速度。

网络信息安全是一个关系到互联网能否正常发展和使用,关系到国家安全和主权、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。

但安全不是绝对的安全,而是相对的。相对的意义在于安全不是要做到毫无缝隙、滴水不漏,而是让攻击者觉得攻击系统的代价远比他能获得的利益高,这样的话绝大多数的攻击者不愿意做这种事。

一般而言,所谓安全要做到什么地步,是根据使用者所能接受的成本及攻击者可能获得最大利益的平衡点而定的。以目前网络上的常见的安全协议而言:SET(Secure Electronic Transaction)是让信用卡的持卡者可以在网上做安全的信用卡交易,但是对于持卡者的保护却不是很周到。持卡者在这个协议中,若以严格安全观点来看几乎是很弱势,在整个交易结束后,并未获得任何已进行交易的证据,是一个纯以银行的观点设计的协议。或许是银行有完整的审计制度,并且若有这类官司发生有损其声誉,一般除了银行内部的个人行为外,银行不太可能会发生这种欺诈行为。所以当设计一个安全的应用系统时,并不是要做到滴水不漏,而是看看系统的需求及应用范围,及其所能承受的风险,而来定义出此系统所需的功能,及需达到的功能。所以,一个安全系统首先考虑较为基本的安全问题,其他问题如密码组件实体安全部分,可以待实行之后在后续的系统建设和维护中完善。

1.2　网络安全的典型案例

1.2.1　国外网络安全的案例

网络与信息系统在变成“金库”，当然就会吸引大批合法或非法的“掏金者”，所以网络信息的安全与保密问题显得越来越重要。现在，几乎每天都有各种各样的“黑客”故事：

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 CITYBANK 银行发动了一连串攻击，通过电子转账方式，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”（正义的化身）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。

1996 年 9 月 18 日，“黑客”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”（CIA-Central Intelligence Agency 变 CSA-Central Stupid Agency），用以讽刺“中央情报局”在办一些事情时是无能的。

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，迫使美国国防部一度关闭了其他 80 多个军方网址。

1996 年 12 月 29 日，美国空军的全球网页完全变了样，其中空军介绍、新闻发布等内容被替换成一段简短的黄色录像，且声称美国政府所说的一切都是谎言。

1998 年 11 月，美国康乃尔大学的学生 Morris 编制的名为蠕虫的计算机病毒通过因特网传播，致使网络中约 7000 台计算机被传染，造成经济损失约 1 亿美元。

2000 年春节期间“黑客”攻击以 Yahoo 和新浪等为代表的国内外著名网站，造成重大经济损失。

2000 年 3 月 6 日晚 6 时 50 分，美国白宫网站主页被黑：在白宫上空飘扬的美国国旗竟变成了骷髅头的海盗旗；在克林顿与戈尔的合影中，戈尔成了独眼龙。更可笑的是，几分钟后白宫上悬挂的旗帜又摇身一变成了一美女剪影，而戈尔则变成了一个汉堡包。此后不久，主页又被“黑客”修改，在美国国旗位置出现了三排歪歪扭扭的红色字体：Hackers was here（“黑客”到此一游）。

1.2.2　国内网络安全的案例

1999 年 8 月 8 日，台湾“监察院”宣布其电脑网站被署名“中国黑客”入侵，原内容被另外的中英文“世界只有一个中国，也只需要一个中国”的字样所覆盖。该院立即关闭网页。当晚台湾“黑客”成功侵入铁道部的网页，将中国国歌及国旗改为所谓“中华民国”的“国歌”及“国旗”，并换以“光复”内容。

1997 年 12 月 19 日至 1999 年 8 月 18 日：有人先后 19 次入侵某证券公司上海分公司电脑数据库，非法操作股票价格，累计挪用金额 1290 万元。

1998 年 2 月 25 日，“黑客”入侵中国公众多媒体通信网广州蓝天 bbs 系统并得到系统的最高权限，系统失控长达 15 小时，为国内首例网上“黑客”案件。

1998 年 9 月 22 日,“黑客”入侵扬州工商银行电脑系统,将 72 万元注入其户头,提出 26 万元,为国内首例利用计算机盗窃银行巨款案件。

1999 年 4 月 16 日,“黑客”入侵中亚信托投资公司上海某证券营业部,造成 340 万元损失。

1999 年 11 月 14 日至 17 日,新疆乌鲁木齐市发生首起针对银行自动提款机的“黑客”案件,用户的信用卡被盗 1.799 万元。

1999 年 11 月 23 日,银行内部人员通过更改程序,用虚假信息从本溪某银行提取出 86 万元。

1998 年 8 月 22 日,江西省中国公用多媒体信息网(169 台)被电脑“黑客”攻击,整个系统瘫痪。

1998 年 4 月 25 日下午 5 时 30 分左右,神秘的电脑“黑客”非法侵入中国公众多媒体信息网(CHINANET)贵州站点的 WWW 主机,将“贵州省情”的 WEB 页面改换成一幅不堪入目的淫秽画面。

1998 年 6 月 16 日,“黑客”入侵了上海某信息网的 8 台服务器,破译了网络大部分工作人员的口令和 500 多个合法用户的账号和密码,其中包括 2 台服务器上超级用户的账号和密码。

1998 年 10 月 27 日,刚刚开通的、由中国人权研究会与中国国际互联网新闻中心联合创办的“中国人权研究会”网页,被“黑客”严重篡改。

2000 年 2 月 1 日,“黑客”攻击了大连市赛伯网络服务有限公司,造成经济损失 20 多万元。

2000 年 2 月 1 日、2 日,中国公共多媒体信息网兰州节点——“飞天网景信息港”遭到“黑客”攻击。

2000 年 3 月 2 日,“黑客”攻击世纪龙公司 21CN 网站。

2000 年 3 月 6 日至 8 日,“黑客”攻击实华开 EC123 网站达 16 次,同一时期,号称全球最大的中文网上书店“当当书店”也多次遭到“黑客”攻击。

2000 年 3 月 8 日,山西日报国际互联网站遭到“黑客”数次攻击,被迫关机,这是国内首例“黑客”攻击省级党报网站事件。

2000 年 3 月 8 日,“黑客”攻击国内最大的电子邮局——拥有 200 万用户的广州 163,系统无法正常登录。

2000 年 3 月 9 日,IT163.com——全国网上连锁商城遭到“黑客”袭击,网站页面文件全部被删除,各种数据库遭到不同程度破坏,网站无法运行,15 日才恢复正常,损失巨大。

2000 年 3 月 25 日,重庆某银行储户的个人账户被非法提走 5 万余元。

2000 年 6 月 11 日、12 日,中国香港特区政府互联网服务指南主页遭到“黑客”入侵,服务被迫暂停。

1.3 网络信息安全概述

网络信息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。

严格地说，网络信息安全不仅仅是一种手段和方法，更准确地说应是一种方法论和系统的思想，是指导我们如何从事网络安全工作的总体模式。

信息是资产。信息与其他资产一样应当受到保护。信息安全的作用是保护信息不受大范围威胁或干扰，使业务能够顺畅，减少损失及提供最大的投资回报和商机。

信息有多种存在方式：信息可以写在纸上、存储在电子文档里，也可以用邮递或电子手段发送，可以通过电影放映或者在说话中提到。

信息在计算机里，无论什么体现方式，均是存储成数据形式。数据和信息两者既有联系又有区别，是同一类问题的不同内涵拓展。数据是指测量值，而信息则是被赋予某种语义的数据，也就是说，信息是对数据理解之后的结果。数据是信息的前奏和基础，信息则是数据的归宿和终结。

所以，网络的安全就是网络中数据的安全，最终表现为网络信息安全。网络信息安全是广义上的网络安全。

1.3.1　网络信息安全内涵

计算机安全的主要目标是对网络系统的硬件、软件及其系统中的数据进行保护，使其不受偶然的或者恶意的破坏、更改、泄露，保证系统连续、可靠、正常地工作，网络服务不中断。其安全就是一个组织机构本身的安全。

网络安全从其本质上来讲就是网络上的信息安全，它涉及的领域相当广泛。这是因为在目前的公用通信网络中存在着各种各样的安全漏洞和威胁。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所要研究的领域。下面给出网络安全的一个通用定义。

网络安全是指网络系统的硬件、软件及系统中的数据受到保护，不因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。

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、抵赖等手段对用户的利益和隐私造成损害和侵犯，同时也希望当用户的信息保存在某个计算机系统上时，不受其他非法用户的非授权访问和破坏。

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，避免其通过网络泄露，避免由于这类信息的泄露对社会产生危害，对国家造成巨大的经济损失。

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。

网络安全在不同的环境和应用会得到不同的解释。

运行系统安全，即保证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，计算机结果设计上的安全性考虑，硬件系统的可靠安全运行，计算机操作系统和应用软件的安全，数据库系统的安全，电磁信息泄露的防护等。它侧重于保

证系统正常的运行，避免因为系统的崩溃和损坏而对系统存储、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，本质上是保护系统的合法操作和正常运行。

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，数据加密等。

网络上信息传播的安全，即信息传播后果的安全。其中包括信息过滤，不良信息的过滤等。该安全侧重于防止和控制非法、有害的信息进行传播，同时避免公用通信网络上大量自由传输的信息失控。其本质是维护道德、法规或国家利益。

网络上信息内容的安全，即我们讨论的狭义的“信息安全”。它侧重于保护信息的保密性、真实性和完整性。同时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。

显而易见，网络安全与其所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时或者静态存放时不被非授权用户非法访问，但授权用户却可以访问。显然，网络安全、信息安全和系统安全的研究领域是相互交叉和紧密相连的。

1.3.2 网络安全的技术特征

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、可控性、不可抵赖性等方面。

(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有三种：抗毁性、生存性和有效性。

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。

(2) 可用性：这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。

(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。

(4) 完整性：完整性是网络信息未经授权不能进行改变的特性，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、正确存储和传输。

完整性与保密性不同，保密性要求信息不被泄露给未授权的人，而完整性则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：设备故障、误码(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)、人为攻击、计算机病毒等。

(5) 不可抵赖性：也称不可否认性，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。

1.3.3　网络的安全威胁

计算机网络的发展,使信息共享应用日益广泛与深入。但是信息在公共通信网络上存储、共享和传输,会被非法窃听、截取、篡改或毁坏而导致不可估量的损失。尤其是银行系统、商业系统、管理部门、政府或军事领域对公共通信网络中的存储与传输的数据安全问题更为关注。如果因为安全因素使得不敢把信息放进 Internet 这样的公共网络,那么办公效率及资源的利用率都会受到影响,甚至使得人们丧失了对 Internet 及信息高速公路的信赖。

事物总是辩证的,一方面,网络提供了资源的共享性,用户使用的方便性,通过分布式处理提高了系统效率和可靠性,并且还具有可扩充性。另一方面,正是这些特点增加了网络受攻击的可能性。对网络的威胁来自很多方面,并且随着时间的变化而变化。网络威胁是指对网络构成威胁的用户、事物、想法、软件等。网络威胁会利用系统暴露的要害或弱点,导致网络信息的保密性、完整性和可用性程度下降,造成不可估量的经济和政治上的损失。威胁有两种:一种是无意的,一种是有意的。无意的威胁包括人为操作错误、设备故障、自然灾害等很多不以人的意志为转移的事件。有意的威胁包括窃听、计算机犯罪等人为的破坏。当前主要的威胁来自以下几个方面:

(1) 自然灾害、意外事故;

(2) 计算机犯罪;

(3) 人为行为,比如使用不当、安全意识差等;

(4) "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、非法链接等;

(5) 内部泄密;

(6) 外部泄密;

(7) 信息丢失;

(8) 电子谍报,比如信息流量分析、信息窃取等;

(9) 信息战;

(10) 网络协议中的缺陷,例如 TCP/IP 协议的安全问题等。

1.3.4　网络安全结构层次

网络安全的结构层次包括:物理安全、安全控制、安全服务和可靠服务,如图 1 - 1 所示。

1) 物理安全

网络安全首先要保障网络上信息的物理安全。物理安全是指在物理介质层次上对存储和传输的信息的安全保护。目前常见的不安全因素(安全威胁或安全风险)包括如下四

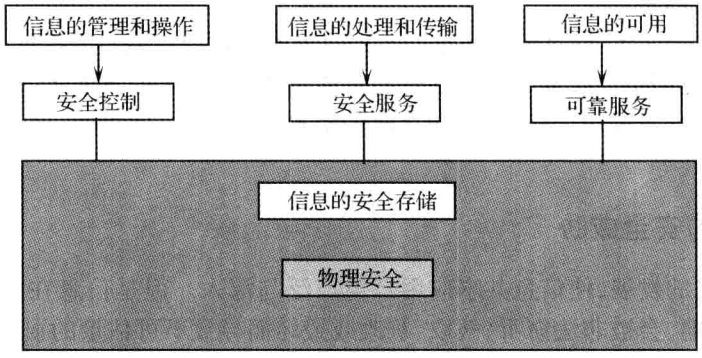


图 1-1 网络安全的结构层次

大类。

(1) 自然灾害(如雷电、地震、火灾、水灾等),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)和意外事故。

特点是:突发性,自然因素性,非针对性。这种安全威胁只破坏信息的完整性和可用性(无损信息的秘密性)。

解决方案是:防护措施,安全制度,数据备份等。

(2) 电磁泄漏(如侦听微机操作过程),产生信息泄漏,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)和痕迹泄露(如口令密钥等保密不善,易于被人发现)。

特点是:难以察觉性,人为实施的故意性,信息的无意泄露性。这种安全威胁只破坏信息的秘密性(无损信息的完整性和可用性)。

解决方案是:辐射防护,屏幕口令,隐藏销毁等。

(3) 操作失误(如删除文件、格式化硬盘、线路拆除等)和意外疏漏(如系统掉电、"死机"等系统崩溃)。

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(无损信息的秘密性)。

解决方案是:状态检测,报警确认,应急恢复等。

(4) 计算机系统机房环境的安全。

特点是:加强机房管理,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,是不可缺少和忽视的组成部分。一方面,研制生产计算机和通信系统的厂商应该在各种软件和硬件系统中充分考虑到系统所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。

2) 安全控制

安全控制是指在微机操作系统和网络通信设备上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的初步的安全保护。可以分为三个层次。

(1) 微机操作系统的安全控制。如用户开机键入的口令,对文件的读写存取的控制。

主要用于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。在网络环境下对来自其他机器的网络通信进程进行安全控制。主要包括:身份认证、客户权限设置与判别、审计日志等,如 UNIX, Windows95/NT 的网络安全措施。

(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监测和控制。主要通过网管软件或路由器配置实现。

可见,安全控制主要是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的功能和信息保护,仍然存在着很多漏洞和问题。但由于实际情况的限制,很难对此进行弥补和更改。

3) 安全服务

安全服务是指在应用层对信息的保密性、完整性和来源真实性进行保护和鉴别,满足用户的安全需求,防止和抵御各种安全威胁和攻击手段。这是对现有操作系统和通信网络的安全漏洞和问题的弥补和完善。

安全服务包括:安全机制、安全链接、安全协议和安全策略。

(1) 安全机制。安全机制是利用密码算法对重要而敏感的信息进行处理。包括:加密/解密,数字签名/签名验证,信息认证。安全机制是安全服务乃至整个安全系统的核心和关键。现代密码学的理论和技术在安全机制的设计中具有重要的作用。

(2) 安全链接。安全链接是在安全处理前与网络通信方之间的链接过程,为安全处理进行必要的准备工作。主要包括:会话密钥的分配和生成及身份验证。

(3) 安全协议。安全协议是多个使用方为完成某些任务所采取的一系列有序步骤。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不信任的通信方能够相互配合,并通过安全链接和安全机制的实现保证通信过程的安全性、可靠性和公平性。

(4) 安全策略。安全策略是安全体制、安全链接和安全协议的有机组合方式,是系统安全性的完整的解决方案。安全策略决定了信息安全系统的整体安全性和实用性。不同的通信系统和具体的应用环境决定不同的安全策略。

另外,安全设备是存储密钥、口令、权限、审计记录等安全信息的硬件介质和载体,以及存储和运行安全信息系统的设备,如具有防火墙功能的路由器,具有密钥分配和认证功能的安全服务器等。安全设备自身的安全防护也是必不可少的。

1.3.5　网络安全的关键技术

从广义来说,凡是涉及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。

目前流行的 5 种安全技术是:

(1) 密码学;

(2) 防火墙;

(3) 病毒和预防病毒技术;

(4) 操作系统安全;

(5) 入侵检测。