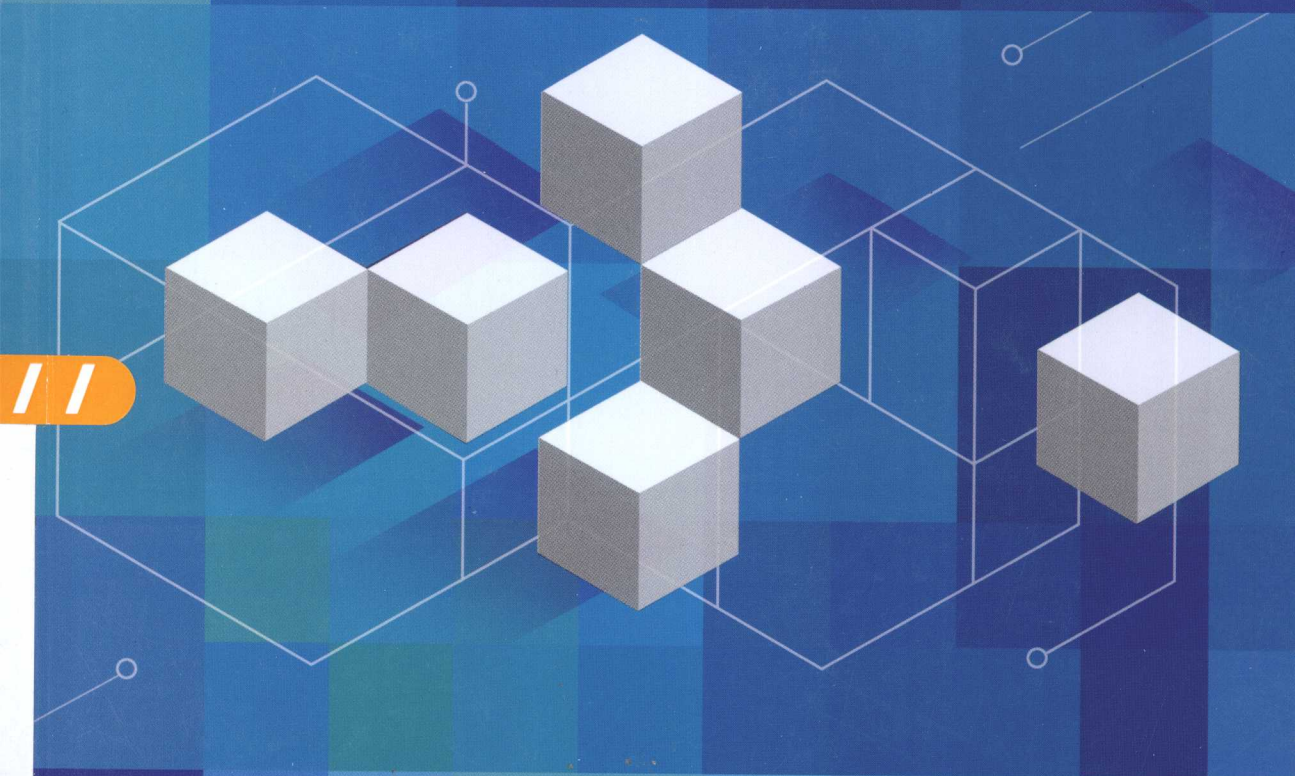
网络安全的特性、机制与评价

◎ 田立勤 著



清华大学出版社 · 北京交通大学出版社

网络安全的特性、机制与评价

田立勤 著

清华大学出版社
北京交通大学出版社
·北京·

内 容 简 介

网络安全是计算机和通信领域很重要的研究方向之一，而网络安全特性及其实现机制是保障网络安全中的重要研究内容。本书分为九章，以保障计算机网络的安全特性为主线，论述实现计算机网络系统安全、计算机网络数据安全和计算机网络用户安全的三个方面的八大特性与机制，并对各个实现机制的意义、定义、导致出现安全问题的原因、评价标准、解决问题的基本思路、分类和实例等进行了详细的论述和分析。

本书全面系统地展示了网络安全特性及其实现机制的研究内容和最新成果，具有完整性、实用性和学术性。非常适合我国计算机网络和通信领域的教学、科研工作和工程应用参考。既可以供计算机、通信、电子、信息等相关专业的科研人员、研究生和大学高年级学生作为教材或教学参考书，也可以供计算机网络研究开发人员、网络运营商等网络工程技术人员参考。

图书在版编目（CIP）数据

网络安全的特性、机制与评价 / 田立勤著. —北京：清华大学出版社；北京交通大学出版社，2013.6
ISBN 978-7-5121-1435-7

Ⅰ. ① 网… Ⅱ. ① 田… Ⅲ. ① 计算机网络-安全技术-高等学校-教材
Ⅳ. ① TP393.08

中国版本图书馆 CIP 数据核字（2013）第 074153 号

责任编辑：谭文芳
出版发行：清 华 大 学 出 版 社　　邮编：100084　　电话：010-62776969
　　北京交通大学出版社　　邮编：100044　　电话：010-51686414
印 刷 者：北京泽宇印刷有限公司
经　　销：全国新华书店
开　　本：175×245　　印张：19.25　　字数：428 千字
版　　次：2013 年 6 月第 1 版　　2013 年 6 月第 1 次印刷
书　　号：ISBN 978-7-5121-1435-7 / TP・737
印　　数：1～800 册　　定价：48.00 元

前　言

背景

随着因特网、物联网的迅猛发展，信息技术在人类社会生活各方面得到广泛应用，信息网络的基础性、全局性作用日益增强。目前网络安全问题已经上升到关系国家主权和安全的高度，成为影响社会经济可持续发展的重要因素。信息通信技术的演进和发展使网络信息安全的内涵不断延伸，从最初的信息保密性发展到信息的完整性、可用性和不可否认性，进而发展到系统服务的安全性，包括网络的可靠性、可维护性、可用性、可控性及行为的可信性等，随之出现了多种不同的安全防范机制，如防火墙、入侵检测和防病毒等。虽然安全防范的技术在不断增强增多，但恶意攻击和恶意程序的破坏却并没有因此而减少或减弱。为保证信息安全，人们只好把防火墙、入侵检测、病毒防范等做得越来越复杂，但随着维护与管理复杂度的增加，整个信息系统变得更加复杂和难以维护，也使得信息系统的使用效率大大降低，因此网络正面临着严峻的安全挑战。网络的安全特性是描述和评价网络安全的重要指标，它为网络安全的定量评价与分析提供基础，其机制的实现是保障网络安全的主要途径，所以网络安全特性的准确含义、实现思路、评价标准、具体实现机制及机制的评价与改进成为提高网络安全的重要内容。

本书以保障计算机网络的安全特性为主线，论述实现计算机网络系统安全、计算机网络数据安全和计算机网络用户安全的三个方面的八大特性与机制（即，计算机网络的可靠性、计算机网络的可用性、计算机网络的可控性，用户身份可鉴别性、用户行为可信性和用户不可抵赖性，网络数据的保密性、网络数据的完整性），并对各个实现机制的意义、定义、导致出现安全问题的原因、评价标准、解决问题的基本思路、分类和实例等进行了详细的论述和分析。

本书特点与读者对象

本书具有以下鲜明特色。

（1）完整性：内容丰富全面，结构合理，体系完整，对网络安全特性与机制进行全面和系统的介绍。

（2）实用性：结合当前网络环境的特点，将网络安全特性与机制应用于云计算等新型网络应用中，给出具体的应用实例，具有很强的实用性。

（3）学术性：本书具有一定的理论高度和学术价值，书中大部分内容取材于作者近期已在国际、国内学术期刊发表的论文，全面展示了网络安全特性与机制最新的科研成果，具有很高的学术参考价值。

本书非常适合我国计算机网络和通信领域的教学、科研工作和工程应用参考。既可以供计算机、通信、电子、信息等相关专业的科研人员、研究生和大学高年级学生作为教材或教学参考书，也可以供计算机网络研究开发人员、网络运营商等网络工程技术人员参考。

致谢

作者的研究工作得到 973 计划项目(No. 2011CB311809)，国家自然科学基金（No.61163050），新世纪优秀人才（NCET-10-0101），中央高校基本科研项目（No. 3142013098）和青海省科技项目（No. 2012-N-525）的资助，在此表示深深的谢意！

本书的研究工作大都是在我的导师林闯教授的指导下完成的，现在所取得的成绩离不开导师对我的教诲和帮助；另外，王晓菊老师对本书进行了细致的校对，谭文芳老师在本书的写作过程中做了大量细致辛苦的工作，对此一并表示衷心的感谢！。

由于作者水平所限，加之网络安全的研究仍处于不断的发展和变化之中，书中错误和不足之处在所难免，恳请专家、读者指正。

作　者

2013 年 3 月

目　录

第一部分 网络系统的安全特性、机制与评价

第三部分 用户的安全特性、机制与评价

第1章

网络安全特性概述

1.1 网络安全与网络安全特性概述

随着因特网、物联网的迅猛发展和信息技术在人类社会生活各方面的广泛应用，信息网络的基础性、全局性作用得到日益增强。网络已发展成为建设和谐社会的一项重要基础设施，它在通信、交通、金融、应急服务、能源调度、电力调度等方面发挥重要作用，如图 1-1 所示。

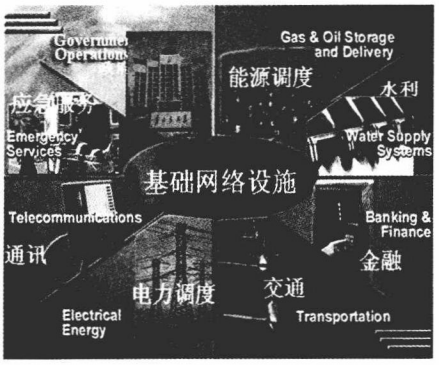


图 1-1　计算机网络的基础作用

网络安全是网络应用中重点需要解决的问题，目前网络安全已经上升到关系国家主权和安全的高度，成为影响社会经济可持续发展的重要因素。我国明确提出“加强宽带通信网、数字电视网和下一代互联网等信息基础设施建设，推进三网融合，健全信息安全保障体系”。

随着信息通信技术的演进和发展，网络信息安全的内涵不断延伸，从最初的数据保密性发展到数据的完整性、进而又发展到系统服务的安全性，包括网络的可靠性、可维护性、可用性、可控性，以及用户身份的可鉴别性、不可抵赖性和行为的可信性等，随之出现了多种不同的安全防范机制，如防火墙、入侵检测和防病毒等。虽然安

全防范的技术不断增多增强，但恶意攻击和恶意程序的破坏却并没有因此而减少或减弱。为保证信息安全，人们只好把防火墙、入侵检测、病毒防范等做得越来越复杂，但随着维护与管理复杂度的增加，整个信息系统变得更加复杂和难以维护，也使得信息系统的使用效率大大降低，因此网络正面临着严峻的安全挑战。

网络的安全特性是描述和评价网络安全的重要指标，它为网络安全的定量评价与分析提供基础，其机制的实现是保障网络安全的主要途径，所以网络安全特性的准确含义、实现思路、评价标准、具体实现机制以及机制的好坏成为提高网络安全的重要内容。

1.2 网络安全含义

定义 1.1 网络安全 网络安全泛指网络系统的硬件、软件及其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、更改和泄漏，系统能够连续可靠正常地运行，网络服务不被中断。

网络安全的内容包括系统安全和信息安全两部分。系统安全主要指网络设备的硬件、操作系统和应用软件的安全。信息安全主要指各种信息的存储、传输安全，具体体现在信息的保密性、完整性及不可抵赖性方面。通过采用各种技术和管理措施，使网络系统正常运行，从而确保网络数据的可用性、完整性和保密性。所以，建立网络安全保护措施的目的是确保经过网络传输和交换的数据不会被增加、修改、丢失和泄露等。

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、数论和信息论等多种学科的综合性学科。从内容看，网络安全包括物理实体安全、软件安全、数据安全和安全管理四个方面。

1. 物理实体安全

物理实体安全主要包括以下三个方面内容。

（1）设备安全

设备安全主要包括设备的防盗、防毁、防电磁信息辐射泄漏、防线路截获、抗电磁干扰及电源保护等。

（2）存储介质安全

存储介质安全的目的是保护存储在存储介质上的信息，包括存储介质数据的安全及存储介质本身的安全。

存储介质数据的安全是指对存储介质数据的保护，包括：①存储介质数据的安全删除，包括存储介质的物理销毁（如存储介质粉碎等）和存储介质数据的彻底销毁（如消磁等），防止存储介质数据删除或销毁后被他人恢复而泄露信息；②存储介质数据的防盗，是指防止存储介质数据被非法拷贝等；③存储介质数据的防毁，是指防止意外或故意的破坏使存储介质数据丢失。

（3）环境安全

对系统所在环境的安全保护，可按照国家标准 GB 50173—2008《电子信息系统机房设计规范》和 GB/T 2887—2011《计算机场地通用规范》对网络环境进行安全设置。

2. 软件安全

软件安全又包括两个方面。

一是指软件本身是安全的，不会发生软件故障或者即使发生软件故障，该故障也不是危险的。由于软件安全漏洞带来的各种危害随着软件应用的发展日益严重，因此能有效发现并消除漏洞的软件安全漏洞发现技术也日益受到人们的重视。

二是指保护网络系统中的系统软件与应用软件不被非法复制、篡改和不受病毒的侵害等。例如，将加密技术应用于程序的运行，通过对程序的运行实行加密保护，可以防止软件被非法复制盗版以及软件安全机制被破坏。

3. 数据安全

数据安全主要指保护网络中的数据不被非法存取和破坏，确保其完整性和机密性。数据的完整性是指阻止非法实体对交换数据的修改、插入和删除；数据的保密性是指为了防止网络中各个系统之间交换的数据被截获或被非法存取而造成泄密，提供加密保护。

4. 安全管理

网络安全管理主要是以保护网络安全技术为基础，配以行政手段的管理活动。在安全问题中有相当一部分事件不是因为技术原因而是由于管理原因造成的。例如，管理规章制度的不健全、操作规程不合理和安全事件预防措施不得力等，特别是安全管理人员的误操作或恶意破坏等。只有在采取安全技术的同时，采取有力的安全管理措施才能保证网络的安全性。安全管理的对象是整个系统而不是系统中的某个或某些元素。一般来说，系统的所有构成要素都是管理的对象，从系统内部看，安全管理涉及计算机、网络、操作、人事和信息资源；从外部环境看，安全管理涉及法律、道德、文化传统和社会制度等方面的内容。确保网络安全的措施一般包括采取网络安全保障机制，建立安全管理制度，开展安全审计，进行风险分析等。

1.3　网络安全的辩证观

由于计算机网络安全不是绝对的纯技术或纯管理所能解决的问题，也不是绝对的资金投入越多越安全的问题，只有大家结合所学知识和利用辩证唯物主义理论进行思考和辨析，才能培养正确的计算机网络安全观，下面对常见的安全观点进行辩证分析。