国家出版基金项目
NATIONAL PUBLICATION FOUNDATION

“十二五”
国家重点图书出版规划项目

学术中国 · 院士系列

未来网络创新技术研究系列

网络安全传输与管控技术

兰巨龙　江逸茗　胡宇翔　刘文芬　李玉峰　张建辉　邬江兴　编著

Cyber Secure Transmission and Control Technologies

中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

"十二五"
国家重点图书出版规划项目

学术中国 · 院士系列

未来网络创新技术研究系列

网络安全传输与管控技术

■ 兰巨龙 江逸茗 胡宇翔 刘文芬 李玉峰 张建辉 邬江兴 编著

Cyber Secure Transmission and Control Technologies

人民邮电出版社
北京

图书在版编目（CIP）数据

网络安全传输与管控技术 / 兰巨龙等编著. -- 北京：人民邮电出版社，2016.9
（学术中国. 院士系列. 未来网络创新技术研究系列）
ISBN 978-7-115-42782-3

Ⅰ. ①网… Ⅱ. ①兰… Ⅲ. ①计算机网络－数据传输－研究 Ⅳ. ①TP393.0

中国版本图书馆CIP数据核字(2016)第137998号

内 容 提 要

本书在介绍网络安全传输与管控概念和背景的基础上，对网络安全基础、网络安全传输、网络管控以及网络路由抗毁与自愈的研究现状进行了全面系统的介绍。结合作者对网络安全传输与管控的理解和所从事工作的实践经验，本书最后给出了网络安全管控系统的开发实例。

本书取材新颖、内容翔实、实用性强，反映了国内外网络安全传输与管控技术的现状与未来，适合于从事网络信息安全的广大工程技术人员阅读，也可作为大专院校通信、计算机等专业和相关培训班的教材或教学参考书。

◆ 编　　著　兰巨龙　江逸茗　胡宇翔　刘文芬　李玉峰
　　张建辉　邬江兴
　　责任编辑　代晓丽
　　责任印制　彭志环
◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
　　邮编　100164　　电子邮件　315@ptpress.com.cn
　　网址　http://www.ptpress.com.cn
　　北京圣夫亚美印刷有限公司印刷
◆ 开本：700×1000　1/16
　　印张：22.5　　2016 年 9 月第 1 版
　　字数：441 千字　　2016 年 9 月北京第 1 次印刷

定价：118.00 元

读者服务热线：(010)81055488　印装质量热线：(010)81055316
反盗版热线：(010)81055315

前 言

随着当前网络信息技术水平的高速发展和影响领域的快速拓展，网络已经渗透到每个国家的政治、经济、军事、文化、生活等各个领域，整个社会运转已经与网络密不可分。人类在享受其带来的便捷丰富内容和便捷条件的同时，网络信息的安全问题却日益显现，网络信息的处理、传输、存储面临着严重的威胁和风险，各种暴力、色情等不良信息也在网络空间快速蔓延。因此，网络安全传输与管控技术正日益成为一个具有重大现实意义的研究方向。

网络的安全传输与管控就是要防止通过网络传输的信息数据被故意或偶然地泄露、更改、破坏或使信息被非法辨认、控制，保障网络信息的保密性、完整性、可用性、认证性、可控性、不可抵赖性等安全属性。此外，还必须保证信息传播的安全，也就是指信息传播后果的安全，主要涉及可控性等安全属性，包括信息过滤、信息传播控制、信息引导等。它侧重于防止和控制非法、有害的信息进行传播的后果，避免公用网络上大量自由传输的信息失控。因此，本书以互联网为主要研究对象，介绍信息网络的安全传输和管控技术的相关知识。

本书主要内容包括：第 1 章介绍了网络安全传输与管控技术的研究背景，引入了网络安全传输与管控技术的基本概念，总结了网络安全传输与管控的技术组成和设计目标；第 2 章主要介绍信息网络安全基础，包括信息加密技术、Hash 函数、安全认证协议和信任机制；第 3 章重点介绍了网络安全传输技术，包括防火墙技术、入侵检测技术、主动防御技术和 VPN 技术；第 4 章介绍了网络路由抗毁与自愈技术，包括网络路由抗毁与自愈技术的基本概念和技术路线，介绍了基于该技术的节点势能导向的多下一跳路由协议，以及基于该协议的快速自愈路由系统——势能导向路由器；第 5 章介绍当前的网络安全管控技术，包括网络安全管控架构、网络视频管控技术、流量清洗技术、互联网用户行为分析技术和网络热点发现技术；第 6 章则根据作者所从事工作的实践经验和对信息网络安全管控的理解，给出了网络安全管控系统的开发实例。

本书在编著过程中得到了国家“973”计划项目“可重构信息通信基础网络体系研究”（编号：2012CB315900）和课题“网络组件模型与聚类机制”（编号：

2013CB329104）等的资助。同时，作者在编写第 6 章的过程中参考了国家“863”计划课题“快速自愈路由协议与试验系统”和“面向三网融合的统一安全管控网络”的大量技术资料。

兰巨龙教授负责本书的统筹规划，邬江兴院士与兰巨龙教授编写了第 1 章，刘文芬教授编写了第 2 章，江逸茗博士编写了第 3 章，张建辉副研究员和胡宇翔博士编写了第 4 章，兰巨龙教授和李玉峰副教授编写了第 5 章，胡宇翔博士和李玉峰副教授编写了第 6 章。另外，项目组的王鹏博士以及博士生王志明、魏江宏、张少军，硕士生王文博、古英汉、刘邦舟、席孝强为本书的文字校阅、插图绘制等做了大量工作。

限于作者水平，并且各种网络安全传输与管控技术研究仍在快速发展和完善之中，本书难免存在缺点甚至是错误之处，敬请广大读者批评指正。

作　者

2016 年 4 月

目 录

第1章

网络安全传输与管控概述

1.1 网络空间安全概述

现代信息技术正在朝着网络化、智能化和普适化的方向迈进，人类社会、信息世界和物理世界正在实现全面连通和相互融合，一种全新的人、机、物和谐共生的发展模式正在孕育之中。计算机网络不但是人们享受丰富服务的平台，也是国家政治、经济、军事、外交活动所依赖的重要信息基础设施，已经成为当今信息社会的基石[1]。

根据联合国国际电信联盟（ITU）的定义，网络空间是指“由以下所有或部分要素创建或组成的物理或非物理的领域，这些要素包括计算机、计算机系统、网络及其软件支持、计算机数据、内容数据、流量数据以及用户”。ITU 对网络空间的这一定义涵盖了用户、物理和逻辑 3 个层面的构成要素，具有一定的技术性和科学性。在网络空间安全的定义方面，不同的国家在定义上则会有不同的侧重点，例如，美国同时强调了硬件和软件数据两个层面的安全威胁；英国侧重逻辑层面的应用软件和数据交换、管理；德国则把系统排除在外，仅将焦点对准网络空间的数据处理。这些国家不同的政策倾向，凸显了它们在应对网络空间威胁并制定对策方面的不同侧重。

近几年来，互联网在推动世界经济、政治、文化和社会发展的同时，也产生了新的安全问题。网络犯罪、网络恐怖主义、黑客攻击以及网络战对个人隐私和国家安全的威胁日益凸显。人类在享受互联网带来的方便快捷的同时，网络及其采集、处理、传输、存储的信息也面临着各种安全威胁和风险。由于网络的隐蔽性、快捷性和难以追踪性，通过网络可以轻易跨越传统的国

家边界，对某国重要部门的网站发动攻击，而且威胁的来源很难被追踪，这给国家安全带来了极大的威胁。近年来连续发生了多起产生重大影响的网络安全事件。

2009 年 5 月 19 日，我国 10 多个省市数以亿计的网民遭遇了罕见的“网络塞车”，这是继 2006 年台湾地震造成海底通信光缆中断之后，我国发生的又一起罕见的互联网网络大瘫痪，大多数网民的上网质量都受到了影响。

2010 年 7～9 月的震网病毒（Stuxnet）事件。震网病毒是世界上首个以直接破坏现实世界中工业基础设施为目标的蠕虫病毒，被称为网络“超级武器”。

2011 年诺顿网络犯罪调查报告称：网络犯罪让全球每年损失 3 880 亿美元，远超全球毒品交易总额（2 880 亿美元）。2010 年，全球 4.31 亿人遭受过网络侵害，其中近一半（1.96 亿人）在我国。2011 年，多个国内知名网络社区出现用户信息泄露事件，而在用户数据最为重要的电商领域，也不断传出存在漏洞、用户信息泄露的消息。漏洞报告平台乌云发布漏洞报告称：国内某支付平台的用户信息大量泄露，被用于网络营销，其总量达 1 500 万～2 500 万。

2012 年 2 月 13 日，据称一系列政府网站均遭到了匿名组织的攻击，其中，美国中央情报局官网在周五被黑长达 9 个小时，黑客盗走政府网数万份私人信息。这一组织也曾拦截了伦敦警察与美国联邦调查局之间的一次机密电话会谈，并随后将其上传于网络。

2013 年 6 月 6 日，英国《卫报》和美国《华盛顿邮报》报道，美国国家安全局和联邦调查局于 2007 年启动了一个代号为“棱镜”的秘密监控项目，直接进入美国互联网公司的中心服务器里挖掘数据、收集情报，包括微软、雅虎、谷歌、苹果等在内的 9 家互联网巨头皆卷入其中。据美国中情局前职员爱德华·斯诺登爆料：美国情报机构一直在 9 家美国互联网公司中进行数据挖掘工作，从音/视频、图片、邮件、文档以及连接信息中分析个人的联系方式与行动。监控的类型包括 10 类：信息电邮、即时消息、视频、照片、存储数据、语音聊天、文件传输、视频会议、登录时间、社交网络资料的细节。其中包括两个秘密监视项目；一是监视、监听民众电话的通话记录；二是监视民众的网络活动。

2014 年 1 月 21 日下午 3 点 10 分左右，国内通用顶级域名根服务器忽然出现异常，导致众多知名网站出现 DNS 解析故障，用户无法正常访问。虽然国内访问根服务器很快恢复，但由于 DNS 缓存问题，部分地区用户断网现象仍持续了数小时，至少有 2/3 的国内网站受到影响。微博调查显示，“1·21”全国 DNS 大劫难影响空前。事故发生期间，超过 85%的用户遭遇了 DNS 故障，引发网速变慢和打不开网站的情况。

从上述典型案例可以看出，目前网络空间安全主要面临以下几个威胁。

（1）黑客攻击

黑客攻击，即黑客破解或破坏某个程序、系统及网络安全，是网络攻击中最常见的现象。其攻击手段可分为非破坏性攻击和破坏性攻击两类，前者的目标通常是为了扰乱系统的运行，并不盗窃系统资料；后者是以侵入他人电脑系统、盗窃系统保密信息、破坏目标系统的数据为目的。

（2）有组织的网络犯罪

有组织的网络犯罪是指犯罪分子借助计算机技术，在互联网平台上进行的有组织犯罪活动。与传统的有组织犯罪有所不同，有组织的网络犯罪活动既包含了借助互联网而进行的传统犯罪活动（如洗钱、贩卖人口、贩毒），也包含了互联网所独有的犯罪行为（如窃取信息、金融诈骗等）。

目前，网络犯罪已经成为一个全球性问题，其跨国性、高科技和隐蔽性特征都给国家安全带来了前所未有的挑战，这些威胁主要集中在非传统安全领域。鉴于网络犯罪可能给国家带来的巨大潜在损失，打击网络犯罪应该被纳入国家安全战略统筹考虑，也需要不同国家和不同部门之间的通力合作。

（3）网络恐怖主义

网络恐怖主义包含了两层含义：一是针对信息及计算机系统、程序和数据发起的恐怖袭击；二是利用计算机和互联网作为工具进行的恐怖主义活动，通过制造暴力和对公共设施的毁灭或破坏来制造恐慌和恐怖气氛，从而达到一定的政治目的。

就第一层含义而言，网络攻击的隐蔽性和力量不对称凸显了大国实力的局限性，无论该国的军事实力多么强大，武器多么先进，核武器多么厉害，在不知“敌人”在哪里的情况下，也只能被动防御。从这个角度来说，网络攻击无疑先天就具备了恐怖主义的特质。不过，目前的网络恐怖主义活动主要集中在第二个层面。通过黑客攻击和低级别犯罪等手段，借助互联网组织发起恐怖主义活动，互联网已经成为恐怖主义分子互通有无、相互交流的最重要的场所。除了将网络空间作为通信和交流的媒介之外，恐怖组织还利用网络空间进行理念宣讲、人员招募和激进化培训。目前，恐怖主义的网络攻击还未出现，但是，一旦恐怖组织通过互联网完成了培训和自我激进化，就很有可能将网络空间当作未来一个新的战场。

网络战对国家安全最大的威胁是对基础设施的直接打击。网络技术已经被广泛应用于各个领域，无论是基础设施和信息系统还是复杂的通信网络以及情报数据，都离不开网络技术。一个国家的现代化水平高度依赖信息和网络通信技术的发展，但这无疑也让它更加脆弱。一旦这些网络系统遭到攻击，国家力量就可能被直接削弱，甚至面临着部分或全部瘫痪的风险。一国利用互联网在有价值的网络系统中植入恶意软件，从而以最小的成本从敌方获取所需要的信

息和情报。一旦植入目标系统的木马或“后门”在某个特殊的时期同时被激活（例如政治局势紧张或常规战争爆发），这些情报会对国家安全带来巨大的威胁。

信息战是基于信息操控的一种软网络战，也是心理战的重要组成部分，它旨在通过信息披露来影响敌方的思想和行为，在外交领域也被称为公共外交。20 世纪 90 年代，随着网络媒体的逐渐增多，网络信息战的使用也越来越多。美国对信息战非常重视，在伊拉克战争中就对基地组织进行过信息战。美国为了扭转在伊朗、巴基斯坦、阿富汗和中东地区的不佳形象，也开始越来越多地使用信息战。

综上所述，在全球化、信息化、网络化的背景下，国与国之间的竞争在很大程度上取决于对信息的占有程度和对网络的控制程度。谁拥有制信息权和制网络权，谁就占领了政治、经济、军事、文化的制高点。因此，网络安全传输与管控已成为关系到国家安全和主权、社会稳定、民族文化继承和发扬的重大关键问题。网络安全和防护能力是 21 世纪综合国力、经济竞争实力和生存能力的重要组成部分。网络空间安全作为一项新的全球治理议程，未来达成全球性国际规范面临着很多困难和挑战。网络信息安全问题解决不好将会全方位地危及我国的政治、军事、经济、文化、社会生活的各个方面。

1.2 网络安全传输与管控的概念和目标

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。广义上讲，凡是涉及网络上信息的保密性、完整性、可用性、可靠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[2]。

网络安全传输就是利用安全传输通道传输保密信息或私有信息。网络安全传输问题最初主要指信息的保密性问题，随着信息技术的不断发展，它已经发展到包含信息的完整性、可用性、可控性和不可否认性方面，并在此基础上又衍生出了攻、防、测、控、管、评等多方面的基础理论和实施技术。现在，网络安全已经成为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。

现代信息系统的信息安全建立在信息系统的构造与评估的基础上，其核心问题是密码理论及其应用。建立适当的安全策略并加强安全管理可以保护敏感信息存储和传输过程的安全性。网络安全传输的基本目标如图 1-1 所示。

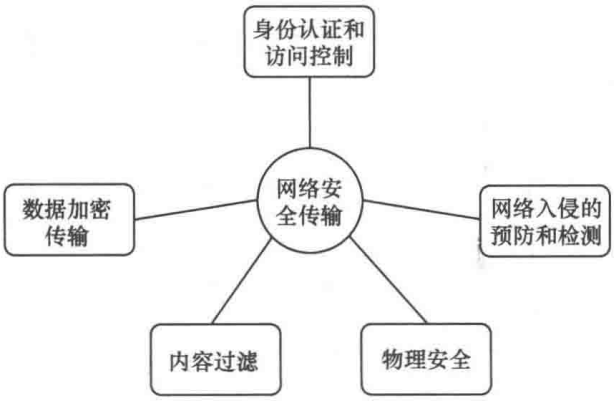

图 1-1　网络安全传输的基本目标

（1）身份认证和访问控制

身份认证的作用是阻止非法用户的不良访问。密码是最常用的用户合法性验证方法，其他方法包括对人体生理特征（如指纹等）的识别、智能卡和令牌等。另外，随着密码学技术的不断发展和进步，新的认证方式不断出现，比如利用用户口令输入的击键特征、基于混沌理论的一次性口令等。

（2）数据加密传输

加密是指对信息进行转换，使得只有使用适当的密钥才能使之还原的过程。信息在网络传输过程中经常会被轻易地截获，需要对传输的信息进行加密。加密的数据又具有不可识别性，因此，通过加密可以保证被截获的数据仍然保持其安全性。

（3）网络入侵的预防和检测

入侵检测系统、虚拟专用网以及防火墙可以保障一个网络不受到非法入侵者的攻击。入侵检测系统可以及时报告潜在的入侵者以及他们试图入侵网络的方式；虚拟专用网允许不同物理位置的用户共享一个跨越公共网络的安全网络连接；防火墙按照预先设定好的策略控制两个网络之间数据分组的进出。

（4）内容过滤

内容过滤是指通过阻止和屏蔽的方式隔绝外部的非法数据。这方面的应用主要包括防病毒软件、垃圾邮件过滤以及地址检测系统等。

（5）物理安全

主要指信息载体的安全保证措施。这方面的安全措施包括电脑锁、缆线等。

各种新兴业务的不断涌现使得网络业务日趋复杂多样，对传统的粗放式网络运行维护和运营模式提出了严峻的挑战，由于缺乏精细化的运营，运营商愈发难以掌控客户的网络行为，无法进行针对性的业务开发和营销。更为严重的是，对于一些不良信息，如非法宣传、网络病毒、网络攻击、垃圾邮件等，由于缺乏有效的识别和管控手段，致使它们通过网络广泛传播、大规模泛滥，对网络的安全

性和可信性造成了严重威胁。为应对上述挑战和威胁，新一代的网络体系架构在设计时都提出了可管、可控、可信的实际需求。

网络管控就是使网络管理者和运营商能够精确识别网络流量中各种业务成分，准确掌握网络流量中业务和用户的组成及变化规律，精细分配网络链路带宽资源，拦截经由网络传播的不良信息，阻断网络上的各类恶意攻击。此外，网络管控的内涵还包括以下几个方面。

- 身份识别与验证。
- 访问控制。对用户的权限进行控制，使之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。

随着网络规模的扩大、网络应用的增加，一些网络应用已无法通过单个管控设备达到控制目的，由此出现了管控网络的概念。管控网络通过管控设备的全网部署及联动机制，在单个管控设备检测到异常的情况下，通过全网联动，快速定位并实时阻断各种业务的非法及不良信息蔓延，缩小影响范围。管控网络由管控平台及管控设备组成。管控设备串接在承载网汇聚层和骨干链路上，具体实施业务识别和管控；管控平台负责对分布于网络各处的管控设备进行维护、管理、策略下发及全网调配部署；管控设备与管控平台之间通过安全协议进行通信。

网络管控的基本目标是对网络信息的传播及其内容具有控制能力，同时能够保障系统依据授权提供服务，使系统在任何时候都不被非授权人使用，对黑客入侵、口令攻击、用户权限非法提升、资源非法使用等攻击行为能够及时采取防范措施。通过进行网络管控，应使网络系统具备以下特性，如图 1-2 所示。

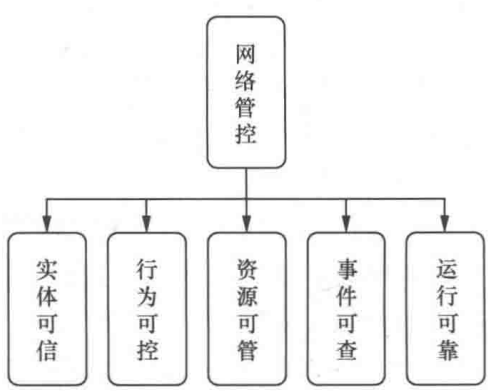

图 1-2　网络管控的基本目标

（1）实体可信

实体指构成信息网络的基本要素，主要包括网络基础设施、软件系统、用户和数据等。实体可信的要求是：保证构建网络的基础设施和软件系统安全可信，没有预留后门或逻辑炸弹；保证接入网络的用户可信，防止恶意用户对系统的攻击破坏；保证在网络上传输、处理、存储的数

据可信，防止搭线窃听，非授权访问或恶意篡改。

（2）行为可控

保证用户行为可控，即保证本地计算机的各种软/硬件资源（例如，内存、中断、I/O 端口、硬盘等硬件设备，文件、目录、进程、系统调用等软件资源）不被非授权使用或不被用于危害本系统及其他系统的安全。保证网络接入可控，即保证用户接入网络应严格受控，用户上网必须经过申请登记和许可。保证网络行为可控，即保证网络上的通信行为受到监视和控制，防止滥用资源、非法外联、网络攻击、非法访问和传播有害信息等恶意事件的发生。

（3）资源可管

保证对路由器、交换机、服务器、邮件系统、目录系统、数据库、域名系统、安全设备、密码设备、密钥参数、交换机端口、IP 地址、用户账号、服务端口等网络资源进行统一管理。

（4）事件可查

保证对网络上的各类违规事件进行监控记录，确保日志记录的完整性，为安全事件稽查、取证提供依据。

（5）运行可靠

保持对信息网络运行可靠性的控制，即保证网络节点在发生自然灾难或遭到硬摧毁时仍能不间断运行，具有容灾抗毁和备份恢复能力。保证能够有效防范病毒和黑客的攻击所引起的网络拥塞、系统崩溃和数据丢失，并具有较强的应急响应和灾难恢复能力。

1.3　网络安全传输与管控技术概述

网络安全传输技术主要分为两类：一类主要用于构建安全的传输环境，包括防火墙技术、入侵检测技术及主动防御技术等；另一类用于构建安全的传输路径，包括密码学相关技术、虚拟专用网技术及网络抗毁技术等。

密码学技术是保护公共网络上所传输的大量敏感信息的不可缺少的工具。密码学技术的基本目标是保证网络信息内容的机密性、完整性和承诺的不可否认性。信息内容的机密性确保信息内容不被非授权获取，一般采用加密技术来实现，包括对称加密技术和公钥加密技术。信息内容的完整性确保信息在传递或存储的过程中没有遭到有意或无意的篡改，一般采用散列技术来实现。信息内容的不可否认性防止了网络实体否认以前的承诺或行为，一般采用数字签名、实体认证、零知识证明等技术实现[3]。然而，在各种新型互联网应用环境下，传统的密码学这种硬安全技术已经无法完全满足网络安全的需求。信任管理这种软安全技术为解