国家出版基金项目
NATIONAL PUBLICATION FOUNDATION

国之重器出版工程
网络强国建设

学术中国·院士系列
未来网络创新技术研究系列

Cyber Secure Transmission and Control Technologies

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

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

国之重器出版工程
网络强国建设

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

Cyber Secure Transmission and Control Technologies

兰巨龙　江逸茗　胡宇翔　刘文芬　李玉峰　张建辉　邬江兴　编著

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，2018.8
（学术中国. 院士系列. 未来网络创新技术研究系列）
国之重器出版工程
ISBN 978-7-115-48766-7

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(2018)第137145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　杨林杰

◆ 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
固安县铭成印刷有限公司印刷

◆ 开本：710×1000　1/16
印张：25　　2018 年 8 月第 1 版
字数：462 千字　　2018 年 8 月河北第 1 次印刷

定价：178.00 元

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

《国之重器出版工程》
编辑委员会

专家委员会委员（按姓氏笔画排列）：

于　全　中国工程院院士

王少萍　“长江学者奖励计划”特聘教授

王建民　清华大学软件学院院长

王哲荣　中国工程院院士

王　越　中国科学院院士、中国工程院院士

尤肖虎　“长江学者奖励计划”特聘教授

邓宗全　中国工程院院士

甘晓华　中国工程院院士

叶培建　中国科学院院士

朱英富　中国工程院院士

朵英贤　中国工程院院士

邬贺铨　中国工程院院士

刘大响　中国工程院院士

刘怡昕　中国工程院院士

刘韵洁　中国工程院院士

孙逢春　中国工程院院士

苏彦庆　“长江学者奖励计划”特聘教授

苏哲子　中国工程院院士

李伯虎　中国工程院院士

李应红　中国科学院院士

李新亚　国家制造强国建设战略咨询委员会委员、中国机械工业联合会副会长

杨德森　中国工程院院士

张宏科　北京交通大学下一代互联网互联设备国家工程实验室主任

陆建勋　中国工程院院士

陆燕荪　国家制造强国建设战略咨询委员会委员、原机械工业部副部长

陈一坚　中国工程院院士

陈懋章　中国工程院院士

金东寒　中国工程院院士

周立伟　中国工程院院士

郑纬民　中国计算机学会原理事长

郑建华　中国科学院院士

屈贤明　国家制造强国建设战略咨询委员会委员、工业和信息化部智能制造专家咨询委员会副主任

项昌乐　“长江学者奖励计划”特聘教授，中国科协书记处书记，北京理工大学党委副书记、副校长

柳百成　中国工程院院士

闻雪友　中国工程院院士

徐德民　中国工程院院士

唐长红　中国工程院院士

黄卫东　“长江学者奖励计划”特聘教授

黄先祥　中国工程院院士

黄　维　中国科学院院士、西北工业大学常务副校长

董景辰　工业和信息化部智能制造专家咨询委员会委员

焦宗夏　“长江学者奖励计划”特聘教授

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重点基础研究发展计划（“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高技术研究发展计划（“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

目 录

第1章

网络安全传输与管控概述

网络安全传输是利用各类信息网络安全技术实现信息的安全传输，包括信息的完整性、可用性、可控性和不可否认性等方面；网络管控技术则是网络管理者准确掌握网络中业务和用户组成、精细分配带宽资源、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的技术。本章从基本概念、目标、技术、发展趋势等方面对网络安全传输与管控技术进行概述。

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年台湾省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月发生了震网病毒（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1 500～2 500万。

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。据美国中央情报局前职员爱德华·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，从音频/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