国防科技图书出版基金

网络与信息安全前沿技术丛书

网络攻击追踪溯源

祝世雄 陈周国 张小松 陈瑞东 著

Traceback Cyber Attacks

国防工业出版社
National Defense Industry Press

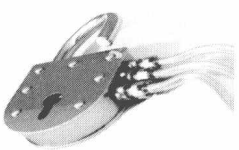
国防科技图书出版基金

网络与信息安全前沿技术丛书

祝世雄　陈周国　张小松　陈瑞东　著

网络攻击追踪溯源

Traceback Cyber Attacks



当网络信息系统遭受攻击时，如何确定攻击者是谁、来自哪里、攻击意图及攻击过程？这一系列问题都需要使用网络攻击追踪溯源这门技术进行解答。在网络空间中有效使用该项技术，就能够定位攻击源头，重构攻击时序，重塑攻击事件，进而能实施针对性的阻截与反制，是网络攻防对抗中的关键技术和重要环节。美国所倡导的网络空间威慑及反制策略中就一直强调其准确定位攻击源的能力，以支撑其全球网络安全战略。本书旨在详细分析攻击追踪溯源所涉及的相关技术及应用，为广大读者全面介绍网络攻击对抗领域中的前沿热点内容，可供相关专业的研究人员阅读和参考。

国防工业出版社
National Defense Industry Press
·北京·

图书在版编目(CIP)数据

网络攻击追踪溯源 / 祝世雄等著. —北京：国防工业出版社，2015.12
（网络与信息安全前沿技术丛书）
ISBN 978-7-118-10572-8

Ⅰ.①网… Ⅱ.①祝… Ⅲ.①计算机网络-安全技术
Ⅳ.①TP393.08

中国版本图书馆 CIP 数据核字(2015)第 268696 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 100048）
北京嘉恒彩色印刷有限责任公司
新华书店经售
*
开本 710×1000　1/16　**印张** 20¾　**字数** 389 千字
2015 年 12 月第 1 版第 1 次印刷　**印数** 1—3000 册　**定价** 99.00 元

致　读　者

本书由国防科技图书出版基金资助出版。

国防科技图书出版工作是国防科技事业的一个重要方面。优秀的国防科技图书既是国防科技成果的一部分，又是国防科技水平的重要标志。为了促进国防科技和武器装备建设事业的发展，加强社会主义物质文明和精神文明建设，培养优秀科技人才，确保国防科技优秀图书的出版，原国防科工委于1988年年初决定每年拨出专款，设立国防科技图书出版基金，成立评审委员会，扶持、审定出版国防科技优秀图书。

国防科技图书出版基金资助的对象是：

1. 在国防科学技术领域中，学术水平高，内容有创见，在学科上居领先地位的基础科学理论图书；在工程技术理论方面有突破的应用科学专著。

2. 学术思想新颖，内容具体、实用，对国防科技和武器装备发展具有较大推动作用的专著；密切结合国防现代化和武器装备现代化需要的高新技术内容的专著。

3. 有重要发展前景和有重大开拓使用价值，密切结合国防现代化和武器装备现代化需要的新工艺、新材料内容的专著。

4. 填补目前我国科技领域空白并具有军事应用前景的薄弱学科和边缘学科的科技图书。

国防科技图书出版基金评审委员会在总装备部的领导下开展工作，负责掌握出版基金的使用方向，评审受理的图书选题，决定资助的图书选题和资助金额，以及决定中断或取消资助等。经评审给予资助的图书，由总装备部国防工业出版社列选出版。

国防科技事业已经取得了举世瞩目的成就。国防科技图书承担着记载和弘扬这些成就，积累和传播科技知识的使命。在改革开放的新形势下，原国防科工委率先设立出版基金，扶持出版科技图书，这是一项具有深远意义的创举。此举势必促使国防科技图书的出版随着国防科技事业的发展更加兴旺。

设立出版基金是一件新生事物，是对出版工作的一项改革。因而，评审工作需

要不断地摸索、认真地总结和及时地改进，这样，才能使有限的基金发挥出巨大的效能。评审工作更需要国防科技和武器装备建设战线广大科技工作者、专家、教授，以及社会各界朋友的热情支持。

让我们携起手来，为祖国昌盛、科技腾飞、出版繁荣而共同奋斗！

国防科技图书出版基金
评审委员会

国防科技图书出版基金
第七届评审委员会组成人员

主任委员	潘银喜			
副主任委员	吴有生	傅兴男	杨崇新	
秘书长	杨崇新			
副秘书长	邢海鹰	谢晓阳		
委员 （按姓氏笔画排序）	才鸿年	马伟明	王小谟	王群书
	甘茂治	甘晓华	卢秉恒	巩水利
	刘泽金	孙秀冬	芮筱亭	李言荣
	李德仁	李德毅	杨　伟	肖志力
	吴宏鑫	张文栋	张信威	陆　军
	陈良惠	房建成	赵万生	赵凤起
	郭云飞	唐志共	陶西平	韩祖南
	傅惠民	魏炳波		

《网络与信息安全前沿技术丛书》编委会

丛书序

网络的触角正伸向全球各个角落，高速发展的信息技术已渗透到各行各业，不仅推动了产业革命、军事革命，还深刻改变着人们的工作、学习和生活方式。然而，在人们享受信息技术带来巨大利益的同时，一次又一次网络信息安全领域发生的重大事件告诫人们，网络与信息安全已直接关系到国家安全和社会稳定，成为我们面临的新的综合性挑战，没有过硬的技术，没有一支高水平的人才队伍，就不可能在未来国际博弈中赢得主动权。

网络与信息安全是一门跨多个领域的综合性学科，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。“道高一尺、魔高一丈”，网络与信息安全技术在博弈中快速发展，出版一套覆盖面较全、反映网络与信息安全方面新知识、新技术、新发展的丛书有着十分迫切的现实需求。

适逢此时，欣闻由我国网络与信息安全领域著名专家何德全院士任编委会主任，以国家保密通信重点实验室为核心，集聚国内信息安全界知名专家学者，潜心数年编写的《网络与信息安全前沿技术丛书》即将分期出版。丛书有如下特点：一是全面系统。丛书涵盖了密码理论与技术、网络与信息安全基础技术、信息安全防御体系，以及近年来快速发展的大数据、云计算、移动互联网、物联网等方面的安全问题。二是适应面宽。丛书既很好地阐述了相关概念、技术原理等基础性知识，又较全面介绍了相关领域前沿技术的最新发展，特别是凝聚了作者

们多年来在该领域从事科技攻关的实践经验，可适应不同层次读者的需求。三是权威性好。编委会由我国网络和信息安全领域权威专家学者组成，各分册作者又均为我国相关领域的知名学者、学术带头人，理论水平高，并有长期科研攻关的丰富积累。

我认为该丛书是一套难得的系统研究网络信息安全技术及应用的综合性书籍，相信丛书的出版既能为公众了解信息安全知识、提升安全防护意识提供很好的选择，又能为从事网络信息安全人才培养的教师和从事相关领域技术攻关的科技工作者提供重要的参考。

作为特别关注网络信息安全技术发展的一名科技人员，我特别感谢何德全院士等专家学者为撰写本书付出的艰辛劳动和做出的重要贡献，愿意向读者推荐该套丛书，并作序。

前言

随着网络的飞速发展，越来越多的传统运作方式正在被低耗、开放、高效的分布式网络应用所替代，网络已经成为人们日常生活中不可缺少的一部分。但是随之而来基于网络的攻击也越演越烈，攻击者利用网络快速而广泛的互联性，使得传统意义上的安全措施基本丧失作用，严重威胁着国家和社会的安全。网络安全威胁给国家和人民生活带来了巨大损失，安全问题已严重制约着网络的发展，并直接威胁国家和社会的稳定。网络安全是任何国家、政府、部门、行业都必须重视的问题，是一个不容忽视的国家安全战略。

网络攻击追踪溯源是指通过网络确定攻击者身份或位置，以及攻击的中间介质，还原攻击路径的技术，美军将其称为“归因（Attribution）”。一般来说，攻击者大都使用伪造 IP 地址、跳板、匿名网络等技术实施网络攻击活动，以逃避追踪，致使防御方难以确定其攻击源头，而不能实施有针对性的防护策略。网络攻击追踪溯源正是在网络空间中实现攻击源定位和攻击时序重构，以有效应对网络攻击，实施针对性的防御和反制，是网络对抗中的关键技术之一，也是网络主动防御中的重要环节。它对于最小化网络攻击的效果，威慑潜在的网络攻击都有着至关重要的作用。

早在 20 世纪末，美国国防部、国土安全部、美国国防部先进研究项目局（Defense Advanced Research Project Agency，DARPA）等部门便开始资助相关技术研究内容，涉及算法、协议及系统应用等。目前美军对网络攻击的追踪和实战能力主要来自美国国防部网络犯罪中心（DC3）及其下属的计算机取证实验室（DCFL），2013 年又与洛克希德·马丁公司、通用动力公司、美国 AIS 公司、CACI 公司等签订了规模达数亿美元的合同，请这些国防承包商进一步研发和改进网络攻击追踪溯源技术、方法和工具。邻国日本在 2005 年启动了国家级网络追踪溯源（IP - Traceback）项目，该项目是集态势感知、溯源和响应为一体的网络攻击溯源系统，并在日本国内实际网络中进行测试，试验结果上报国际互联网工程任务组（The Internet Engineering Task Force，IETF），寻求相关技术的国际标准化。

国内网络攻击追踪溯源相关技术研究起步较晚。目前，市面上还没有系统全面的介绍网络攻击追踪溯源相关内容的图书。在此，我们想通过这本《网络攻击追踪溯源》的出版，向广大科研工作者系统介绍和分析攻击追踪溯源相关技术及其应用，力图为广大读者全面展示网络攻击、追踪溯源等网络对抗中的前沿热点。本书分为网络基础、追踪溯源及追踪溯源防范三部分内容，系统介绍网络架构、攻击行为、攻击追踪溯源以及追踪溯源防范的相关问题和技术内容，并针对不同的网络攻击及应用场景，提出不同层次的追踪溯源。本书内容以计算机网络为网络环境进行介绍分析，其技术原理可适用于移动通信网和工业控制网等更为广泛的网络系统中，内容全面、深入浅出、便于理解，适合于广大技术管理干部、科技人员及大专院校学生作技术参考。

本书共计十章，以通俗的语言全面介绍了网络攻击追踪溯源所涉及的相关问题，重点以互联网为应用场景对网络攻击追踪溯源以及追踪防范相关技术进行了阐述。第 1 章综述网络及网络攻击基础，包括网络基础设施、网络攻击及其相关案例。第 2 章至第 7 章详细介绍网络攻击追踪溯源相关技术内容，包括其概念、发展现状、技术原理、工具软件以及相应系统和案例分析。第 8 章至第 10 章介绍了追踪防范技术，主要介绍匿名通信技术及应用。

网络攻击追踪溯源是一个系统性工程，极具挑战性，也是网络空间综合实力的体现。正如本书中所讲到的，追踪溯源需要通信网络、网络协议、应用系统、态势监测、逆向工程、安全漏洞以及大数据分析等多方面的知识和技术，并能融合应用方可完成准确追踪定位的任务。本书作为此领域书籍编著的初次探索，难免有所遗漏而不能做到面面俱到，我们更期望因此能够吸引更多的技术人员加入到该领域的研究中来。

本书的第 1 章由蒲石、陈周国撰写，第 2、3、6、7 章由陈周国、蒲石撰写，第 4 章由汪小芬、陈周国撰写，第 5 章由陈瑞东撰写，第 8、9、10 章由张小松、陈瑞东撰写。全书由祝世雄、陈周国、蒲石、陈瑞东统稿，祝世雄和陈周国校稿。

保密通信重点实验室张文政研究员、田波研究员、曾兵高工、刘义铭等对本书的出版给与了极大的鼓励和支持，在此表示感谢！全书的编写工作得到了中国电子科技集团公司第三十研究所和保密通信重点实验室的积极支持与配合，对在编著过程中给予协作、帮助的领导、同事一并表示衷心的感谢！

本书的出版得到总装备部国防科技图书出版基金的支持。

由于水平有限，时间仓促，书中难免存在不妥之处，恳请读者批评指正。

编著者

2014 年 9 月 11 日成都

目　录

Contents