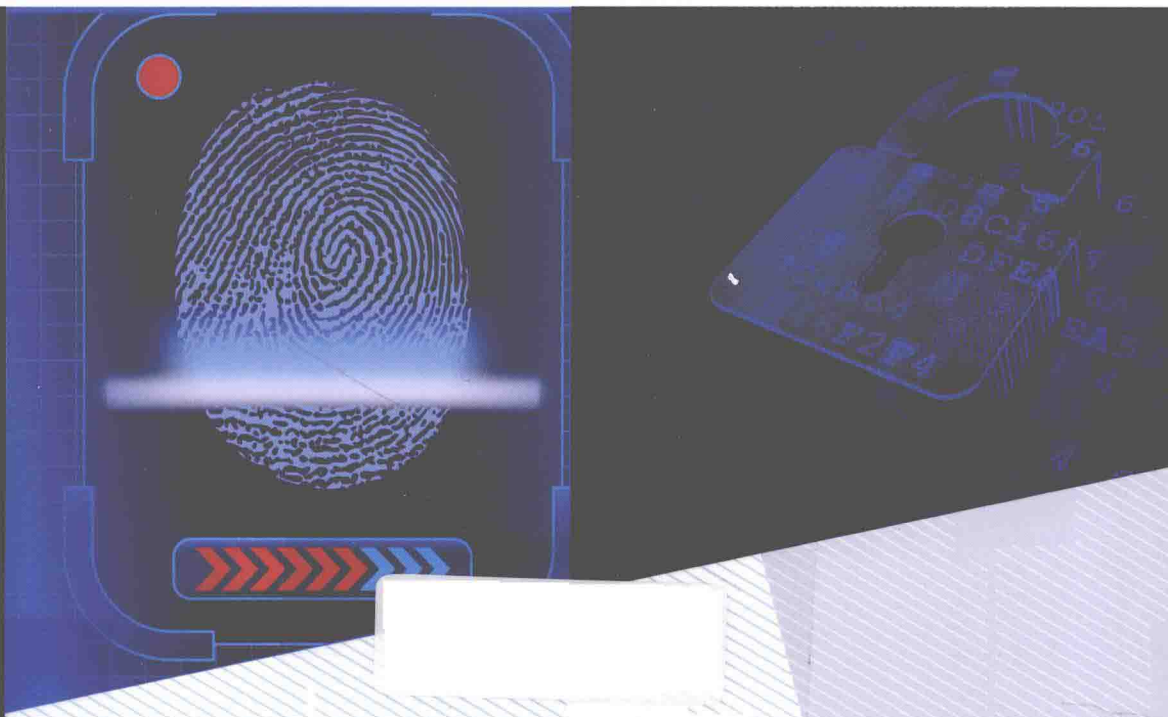
智能科学技术著作丛书

网络安全与“免疫软件人”应用

马占飞 著



科学出版社

智能科学技术著作丛书

网络安全与“免疫软件人”应用

马占飞 著

科学出版社
北京

内 容 简 介

本书在介绍网络安全基础知识、基本理论、典型防御技术以及免疫网络系统等内容的基础上，提出“免疫软件人”的概念及理论体系，并将“免疫软件人”应用到网络信息安全领域，构建基于多“免疫软件人”联盟的网络安全系统，设计基于“免疫软件人”特性的检测器生成模型及算法，并从理论和应用层面对模型及算法进行分析和验证。

本书可供从事计算机科学与技术、人工智能、密码学与信息安全等相关的科研、教学和工程技术人员参考，也可作为网络信息安全专业研究生用书。

图书在版编目(CIP)数据

网络安全与“免疫软件人”应用/马国飞著. —北京：科学出版社，2015.
(智能科学技术著作丛书)

ISBN 978-7-03-044345-8

Ⅰ.①网… Ⅱ.①… Ⅲ.①免疫学-应用-人工智能 Ⅳ.①TP18

中国版本图书馆 CIP 数据核字(2015)第 105621 号

责任编辑：张艳芬 王 苏 / 责任校对：郭瑞芝
责任印制：张 倩 / 封面设计：陈 敬

科 学 出 版 社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

中国科学院印刷厂印刷
科学出版社发行 各地新华书店经销
*
2015 年 5 月第 一 版 开本：720×1000 1/16
2015 年 5 月第一次印刷 印张：21
字数：400 000

定价：98.00 元
(如有印装质量问题，我社负责调换)

《智能科学技术著作丛书》编委会

《智能科学技术著作丛书》序

“智能”是“信息”的精彩结晶，“智能科学技术”是“信息科学技术”的辉煌篇章，“智能化”是“信息化”发展的新动向、新阶段。

“智能科学技术”(intelligence science&technology，IST)是关于“广义智能”的理论方法和应用技术的综合性科学技术领域，其研究对象包括：

- “自然智能”(natural intelligence，NI)，包括“人的智能”(human intelligence，HI)及其他“生物智能”(biological intelligence，BI)。
- “人工智能”(artificial intelligence，AI)，包括“机器智能”(machine intelligence，MI)与“智能机器”(intelligent machine，IM)。
- “集成智能”(integrated intelligence，II)，即“人的智能”与“机器智能”人机互补的集成智能。
- “协同智能”(cooperative intelligence，CI)，指“个体智能”相互协调共生的群体协同智能。
- “分布智能”(distributed intelligence，DI)，如广域信息网、分散大系统的分布式智能。

“人工智能”学科自1956年诞生的，五十余年来，在起伏、曲折的科学征途上不断前进、发展，从狭义人工智能走向广义人工智能，从个体人工智能到群体人工智能，从集中式人工智能到分布式人工智能，在理论方法研究和应用技术开发方面都取得了重大进展。如果说当年“人工智能”学科的诞生是生物科学技术与信息科学技术、系统科学技术的一次成功的结合，那么可以认为，现在“智能科学技术”领域的兴起是在信息化、网络化时代又一次新的多学科交融。

1981年，“中国人工智能学会”(Chinese Association for Artificial Intelligence，CAAI)正式成立，25年来，从艰苦创业到成长壮大，从学习跟踪到自主研发，团结我国广大学者，在“人工智能”的研究开发及应用方面取得了显著的进展，促进了“智能科学技术”的发展。在华夏文化与东方哲学影响下，我国智能科学技术的研究、开发及应用，在学术思想与科学方法上，具有综合性、整体性、协调性的特色，在理论方法研究与应用技术开发方面，取得了具有创新性、开拓性的成果。“智能化”已成为当前新技术、新产品的发展方向和显著标志。

为了适时总结、交流、宣传我国学者在“智能科学技术”领域的研究开发及应用成果，中国人工智能学会与科学出版社合作编辑出版《智能科学技术著作丛书》。需要强调的是，这套丛书将优先出版那些有助于将科学技术转化为生产力以及对社会和国民经济建设有重大作用和应用前景的著作。

我们相信，有广大智能科学技术工作者的积极参与和大力支持，以及编委们的共同努力，《智能科学技术著作丛书》将为繁荣我国智能科学技术事业、增强自

主创新能力、建设创新型国家做出应有的贡献。

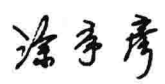
祝《智能科学技术著作丛书》出版，特赋贺诗一首：

智能科技领域广

人机集成智能强

群体智能协同好

智能创新更辉煌



中国人工智能学会荣誉理事长

2005 年 12 月 18 日

序

当人类步入21世纪这一信息网络社会，随之而来的云计算、物联网、微博和微信等新技术、新业务，在信息技术领域以及社会生活等各个方面得到了广泛应用，其带来的安全风险也越来越突出，特别是对信息网络安全防御体系建设将产生深远影响。信息安全的内涵也随之发生了根本性变化，它不仅仅是从一般性的防卫变成了一种非常普通的防范，而且还从一种专门的领域变成了无处不在。

目前，网络安全和信息化已成为事关国家安全和社会发展、事关广大人民群众工作生活的重大战略问题。没有网络安全，信息化发展越快，造成的危害就可能越大；而没有信息化发展，经济社会发展将会滞后，网络安全也没有保障，已有的安全甚至会丧失。因此，加强信息网络安全防御体系建设，积极营造健康向上、和谐有序的网络环境，确保网络良性发展，需要社会各界和广大科研技术人员不懈努力。

内蒙古科技大学马占飞教授在国家自然科学基金、内蒙古自治区自然科学基金等项目的资助下，在多年从事的相关科研、教学工作，以及荣获北京科技大学“优秀博士学位论文”——《基于免疫机理与“软件人”技术的网络安全系统研究》的基础上，撰写了《网络安全与“免疫软件人”应用》一书。该书的出版对研究信息网络安全具有积极的借鉴意义。

“免疫软件人”是一种具有生命特征的、生存并活动于计算机网络世界中的一类免疫智能体，融合了生物免疫系统的相关特性以及“软件人”的理论和技术成果，是计算机网络时代的新技术。

该书在剖析网络安全的基础知识、网络安全的典型防御技术以及免疫网络系统等内容的基础上，介绍了“免疫软件人”的研究背景、科学与技术基础、应用价值，提出了“免疫软件人”的概念及理论体系，包括“免疫软件人”的体系结构、通信机制、迁移方式、联盟机制等关键技术。围绕“免疫软件人”的智能检测特性和网络信息安全防御等关键技术，总结了作者在该领域的研究工作，给出了基于多“免疫软件人”联盟的网络安全系统、基于“免疫软件人”特性的检测器生成模型和算法、基于多“免疫软件人”联盟的网络安全系统设计方法与实现技术，并对模型及其算法进行了深入细致的分析和论述。

该书取材新颖、内容充实、深入浅出、行文流畅，可作为高等院校相关专业的研究生、本科生的教学用书；也可供从事计算机科学与技术、人工智能、密码学与信息安全、通信技术等方面的广大科研、教学、工程技术人员参考。

为了祝贺马占飞的新书面世，赋诗一首：

占飞教授出新书

免疫软件人专著

网络安全应用好

优秀论文奠基础

中国人工智能学会荣誉理事长

北京科技大学计算机与系统科学研究所所长

2014 年 10 月 19 日

前　言

作为20世纪最伟大的科学技术创造之一，互联网已经成为世界各国人民交流的重要工具，真正成为服务用户、互联互通的最好网络互动平台。进入21世纪，以互联网为代表的信息化浪潮席卷世界的每个角落，渗透到经济、政治、科技、文化和国防等各个领域，对人们的生产、工作、学习和生活等产生了全面而深刻的影响，也使世界经济和人类文明跨入了新的历史阶段。然而，伴随着计算机网络技术的飞速发展和互联网的广泛普及，网络信息安全问题日益突出，越来越受到社会各界的高度关注。

网络信息安全是一门涉及计算机科学、生物免疫学、人工智能、通信技术、网络技术、密码技术、应用数学、数论、信息论等多种学科的综合性科学。它主要是指要保护网络系统的硬件、软件及系统中的数据，使其不因偶然的或者恶意的原因而遭到破坏、更改、泄露，使系统连续、可靠、正常地运行，网络服务不中断。然而，在人们广泛利用互联网资源的同时，针对网络和计算机系统的攻击变得越来越普遍，攻击工具与手法也日趋复杂多样。传统的网络安全防御策略(如防火墙技术、加密技术和入侵检测系统)对网络环境下层出不穷的攻击手段和方法缺乏主动性，在某种程度上已无法满足网络信息安全的需求。

目前，网络信息安全作为一个关系国家安全和主权、社会稳定、民族文化继承和发扬的重要问题，其重要性正伴随着全球信息化步伐的加快而越来越明显。因此，如何在推动社会信息化进程中加强网络与信息安全管理，维护互联网各方的根本利益和社会和谐稳定，促进经济社会的持续健康发展，成为信息化时代必须认真解决的一个重大问题。由此可见，我们不能不重视已迫在眉睫的网络信息安全问题。

鉴于此，本书在深入研究和剖析网络信息安全、免疫网络系统、网络入侵检测与防御技术以及软件人理论与技术等研究成果的基础上，将生物免疫系统的机理和特性融入软件人技术之中，提出具有一定自治功能的免疫智能实体——“免疫软件人”，并将“免疫软件人”理论和技术成果引入网络信息安全领域。这为解决当前网络信息安全领域存在的诸多问题提供了崭新的研究思路。该项研究旨在获取理论上先进、技术上实用，能够有效改善和提高现有网络安全防范能力的研究成果，充分体现跨学科特点，不仅具有重要的理论意义和现实意义，而且具有广阔的应用前景。

全书共9章。第1章介绍网络安全的基础知识、网络面临的安全威胁，研究网

络安全的社会意义以及网络安全防范的主要技术措施；第 2 章介绍几种典型的网络安全技术，并构建基于防火墙和入侵检测系统的联动系统；第 3 章介绍免疫学与免疫网络学说，生物免疫系统的基本理论，人工免疫系统相关内容及免疫网络系统等；第 4 章介绍“免疫软件人”概念的来源、科学与技术基础和应用价值等；第 5 章阐述“免疫软件人”的概念及工作机理等；第 6 章阐述“免疫软件人”的体系结构、通信机制、迁移方式、联盟机制、开发平台和安全机制等关键技术；第 7 章架构基于多“免疫软件人”联盟的网络安全系统模型，并设计相应算法等；第 8 章设计一种新型的基于“免疫软件人”特性的检测器自适应生成模型和算法，并对其进行系统的分析和讨论；第 9 章从系统的总体设计目标、功能结构、组件的详细设计方法与实现技术等方面对基于多“免疫软件人”联盟的网络安全系统进行阐述和分析。最后给出本书涉及的中英文词汇索引表、常见网络入侵方法及其分析、互联网信息安全资源网站。

在撰写本书过程中，得到作者主持的国家自然科学基金(61163025)、内蒙古自治区自然科学基金(博士基金)(2010BS0904)、内蒙古自治区高等学校科学研究基金(重点项目)(NJ10162，NJZY07116)等项目的支持和资助，而且以这些项目的研究成果为依托撰写的博士学位论文荣获了北京科技大学的“优秀博士学位论文”，在此深表谢意。

非常感谢在攻读博士研究生期间的导师——北京科技大学郑雪峰教授为课题研究和论文写作给予的悉心指导和无私帮助，同时也要感谢北京科技大学博士生导师涂序彦教授和曾广平教授的帮助与指导，他们提出的“软件人”理论，对本书的研究给予了很大的启迪。感谢巴西坎皮纳斯州立大学的 Leandro Nunes de Castro、美国新墨西哥大学的 Stephanie Forrest 和 Steven Andrew Hofmeyr、美国孟菲斯大学的 Dipankar Dasgupta、英国肯特大学的 Jon Timmis，以及英国伦敦大学国王学院的 Jungwon Kim 和 Peter Bentley 等著名学者，他们都是人工免疫研究领域的拓荒者，为本书的研究无私地提供了大量的参考资料和研究成果。在撰写本书过程中还参阅了很多作者的著作、教材和论文资料，在此表示真诚的谢意。杨树英、马子渊和张涵等对本书文字进行了校对，在此一并表示感谢。

基于免疫学和人工智能的网络信息安全研究在国际上兴起的时间较晚，本书又涉及许多新的知识和研究前沿，尽管作者已经倾注了大量的心血和努力，但是不足之处仍在所难免，恳请各位同仁不吝赐教。

马占飞

2014 年 10 月 8 日

目　　录

第 1 章　网络安全概论

随着网络的互联网协议(Internet protocol,IP)化、宽带化、智能化以及新技术、新业务和新业态的快速发展,计算机网络(computer network)的应用日趋广泛与深入,同时,网络安全问题也显得更加突出和复杂[1-3]。20 世纪 60 年代末期,人们已经认识到计算机系统的脆弱性,并开始进行安全性研究。进入 80 年代,计算机的性能有了很大提高,人们将各个孤立的计算机系统联结起来构成网络,实现相互通信和资源共享。特别是 90 年代,互联网(Internet)持续高速地发展,极大地加快了社会信息化的步伐。借助计算机网络环境,实现了跨地区的电子银行、电子商务、电子政务、电子家务、金融网络、制造资源管理和网络虚拟社区等多种应用。网络的开放性也为信息的窃取、盗用、篡改以及各种扰乱和破坏等提供了可乘之机,使信息在存储、处理和传输等各个环节,都有可能遭到入侵者的攻击或者病毒的危害,造成系统的瘫痪或重要数据的丢失[4]。例如,人们经常会听到有关黑客攻破新的工业安全机制的报道,或是数小时内全世界有数百万台计算机感染病毒陷于瘫痪等。总之,网络安全变得越来越重要,它正在成为一个国家政治、军事、经济以及社会生活正常运行的基础,也必将成为一个国家综合实力的重要体现。从技术角度看,网络安全取决于以下两个方面:一是网络设备的硬件;二是网络设备的操作系统和应用软件。如果一个国家在上述两方面不能够同时拥有自主知识产权,那么该国的网络安全将失去基本保障,其安全性潜在地控制在提供网络设备的国家手中。从理论角度分析,网络安全由密码学和安全协议支持。密码的公钥体制和私钥体制仍将继续共存,它们将根据新的攻击方法进行改进。因此,如何对计算机系统和网络中的各种非法行为进行主动防御和有效抑制,已成为当今网络安全领域亟待解决的重要问题[5-8]。

美国计算机紧急事件反应小组协调中心(Computer Emergency Response Team/Coordination Center,CERT/CC)公布的 1988～2003 年的统计数字显示[9],报告的入侵事件几乎呈指数增加;同时,1995～2007 年以及 2008 年前三季度统计的安全漏洞数量也成倍增长,如图 1.1 和图 1.2 所示。

据美国《金融时报》报道,现在平均每 20s 就发生一次入侵计算机互联网的事件;超过 1/3 的互联网防火墙(firewall)曾被攻破。全世界每年由于信息系统的脆弱性而导致的经济损失高达数十亿美元,并且逐年上升。世界互联网的安全状况尚且如此,国内的网络安全状况更令人担忧。很多信息安全方面的专家均认为,我国有网络,但是没有安全的网络。由此看来,我们不能不重视已迫在眉睫的网

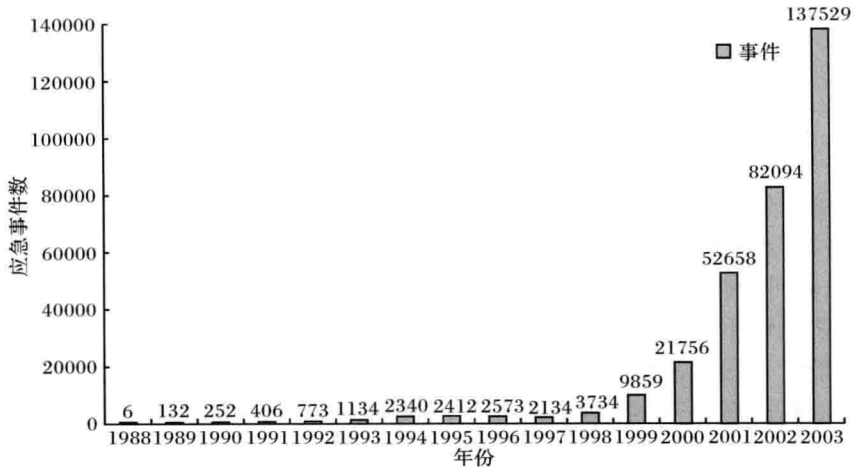


图 1.1 CERT/CC 历年应急事件示意图

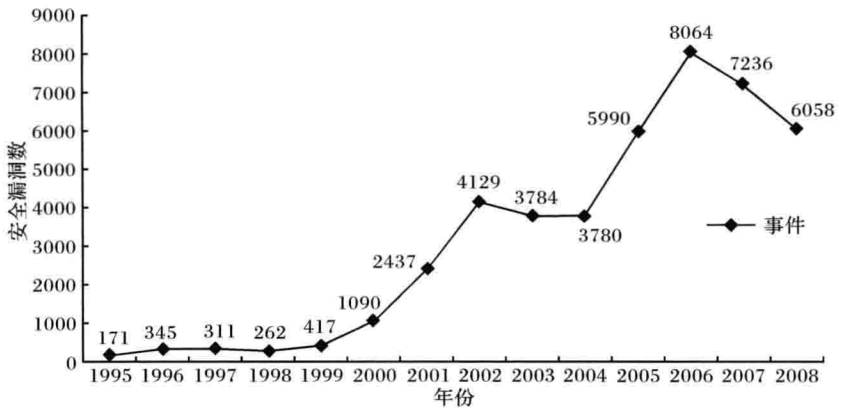


图 1.2 CERT/CC 历年安全漏洞报告

络安全问题。在这种环境下，网络入侵检测与防御技术成为网络信息安全领域研究的热点和重点[10-12]。

近几年，入侵检测(intrusion detection，ID)技术作为一种动态响应技术受到来自政府、研究机构和高等院校等多方面的极大关注。美国国防部高级研究计划局(Defense Advanced Research Projects Agency，DARPA)出巨资资助了一系列入侵检测研究项目[13]。日本、德国等国的政府已拨巨款开展了信息安全方面的研究。我国在“九五”末期紧急启动了 863 信息安全应急计划。“十五”期间，科技部又在 973 计划、863 计划、国家科技攻关计划和科技创新基金计划以及国家自然科学基金中对信息安全技术的研究和开发进行了专项扶持。各大高等院校和科研