网络与信息安全前沿技术丛书

网络安全预警防御技术

主编 姚淑萍　副主编 彭武 吴丹

The Early-warning and Defense Technology of Network Security

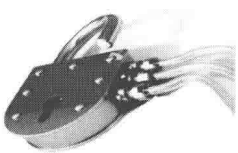
国防工业出版社
National Defense Industry Press

网络与信息安全前沿技术丛书

主　编　姚淑萍
副主编　彭　武　吴　丹
编　著　胡　鹤　王小静　陈君华

网络安全预警防御技术

The Early-warning and Defense Technology of Network Security



网络安全预警防御是一个具有前沿性的研究方向。针对大规模网络安全预警系统研究，急需解决两个问题：一是如何由局部发生的网络攻击评估其对全局的影响；二是如何预测网络攻击方下一步可能采取的行动。以上问题，主要涉及网络攻击意图识别、网络安全态势感知和网络安全协同防护等关键技术。

希望本书所介绍的新原理、新技术能对从事网络安全研究与开发的专业技术人员起到参考作用，也希望对信息安全感兴趣的用户能从中了解预警防御在网络安全防护体系中的重要地位，并获得他们需要的信息。

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

图书在版编目(CIP)数据

网络安全预警防御技术 / 姚淑萍主编. —北京：
国防工业出版社,2015.11
(网络与信息安全前沿技术丛书)
ISBN 978-7-118-10450-9

Ⅰ.①网… Ⅱ.①姚… 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 266147 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** 12　**字数** 227 千字
2015 年 11 月第 1 版第 1 次印刷　**印数** 1—3000 册　**定价** 76.00 元

国防书店:(010)88540777　　发行邮购:(010)88540776
发行传真:(010)88540755　　发行业务:(010)88540717

《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

随着网络应用的快速扩展，网络安全威胁也日益严重，各种攻击的力度、智能化和持续性日益增长，网络面临的安全威胁呈现出了新态势。在这种环境下，快速而准确的预警防御能力对网络安全而言至关重要。

这里所谓的预警防御，是指在实时监控网络攻击的基础上，通过识别网络攻击意图，综合评估网络安全状态并预测其发展趋势，力争在攻击实施的早期阶段发出警报，并提前采取适当的手段予以防御，以尽可能在攻击未产生实质性危害时加以遏制，将损失降到最低。

网络攻击预警是一个具有前沿性的研究方向，国内外在该方面的研究已经取得了很大进展。目前，针对大规模网络安全预警系统研究，急需解决两个问题：一是如何由局部发生的网络攻击评估其对全局的影响；二是如何预测网络攻击方下一步可能采取的行动。以上问题，主要涉及网络攻击意图识别、网络安全态势感知和网络安全协同防护等关键技术。本书旨在反映我们这些年在以上技术领域的研究成果。

希望本书所介绍的新原理、新技术能对从事网络安全研究与开发的专业技术人员起到参考作用，也希望对信息安全感兴趣的用户能从中了解预警防御在网络安全防护体系中的重要地位，并获得他们需要的信息。

本书是集体劳动的结晶，主要内容取自我本人及我们实验室近年来毕业的5位博士研究生的博士学位论文。这5位博士研究生分别是王小静、陈君华、彭武、胡鹤和吴丹，他们的成果分别体现在第3、4、5、7章中。可以说，没有他们的创造性成果，也就没有本书的面世！

值本书出版之际，衷心感谢我的导师胡昌振教授对出版工作的鼎力相助。

书中观点仅是一家之言，谬误在所难免，诚请广大读者批评指正。

姚淑萍

2015年9月

目　录

第1章 导论

自20世纪70年代美国建立ARPANET以来，互联网经历了四十多年的发展，发生了翻天覆地的变化，已经由最初的科研网络逐步演变成为与现实社会形成全息映射的网络空间，该空间正以强大的吸引力聚合着人口资源[1,2]。随着网络应用的快速扩展，网络安全威胁也日益严重，美国、俄罗斯、德国成为全球三大恶意主机的所在国。在命令和控制服务器的总数方面，中国、美国和俄罗斯则占据前三甲[3]。各种攻击的攻击力度、智能化和持续性日益增长，网络面临的安全威胁呈现出了新态势。

1.1 网络安全威胁态势分析

知名信息安全厂商卡巴斯基实验室曾在2013年年初时，对2013年网络重大安全威胁做出预测，指出未来一年继续增长的针对性攻击、网络间谍攻击和国家级网络攻击将呈现加剧形式。正如其言，自2013年以来的安全形势不容乐观，主要呈现出以下特点。

1.1.1 DDoS攻击层出不穷，规模与日俱增

时至今日，网络的威胁已不再是恶作剧，而是以利益驱动的定向攻击。随着这种安全形势的演进，DDoS攻击也在不断发生变化，发生频率与手法不断提高，依然是目前最有效的网络恶意攻击形式之一。

1.1.2 APT攻击攻势不减，破坏力强

APT攻击是一类特定的攻击，指的是为了获取某个组织甚至是国家的重要信息，有针对性地进行的一系列攻击行为。其主要特点是来自于组织、有特定目标、持续时间极长。这一特点充分体现了APT攻击的危险性，它主要是有组织地针对国家重要的基础设施和单位进行，而且具有持续性，可长达数年。这种持续性使攻击者能够长期潜伏，直至收集到重要情报。

2013 年，APT 攻击的发展趋势是攻击更有针对性、更有破坏力，而对其判断却越来越困难，需要综合社会、政治、经济、技术等多重指标进行评估和分析目标，传统的防护手段已经失效，网络安全面临着前所未有的挑战。

1.1.3 大数据依然是网络攻击的显著目标

“大数据（Big Data）”是伴随虚拟技术、云计算、物联网和数据中心等的发展而产生的。大数据应用的普及进一步促进了信息数据的跨域、跨境流动，涉及更多的隐含价值和敏感内容。它不仅仅是数据量的简单刻画，更主要的是指数据正在成为一种资产。美国将大数据定义为“未来的新石油”。

大数据的价值决定了它必然是黑客攻击的首选目标。大数据时代的到来使信息安全的建设面临着新的挑战和要求。

1.1.4 “棱镜门”事件使网络安全上升到了国家级层面

棱镜（Prism），是一项由美国国家安全局负责主导实施的绝密电子监听计划。这项计划主要内容，就是允许国家安全局通过各种手段，对美国公民的各种网络通信内容、网络存储信息文档等资料进行深度的监听；对其他国家网络进行特定的入侵和情报收集。

2013 年的“棱镜门”事件表明，信息安全已成国家安全新战略制高点，网络与信息安全应上升为国家战略。

1.2 预警防御相关技术研究现状分析

为应对日益复杂化、智能化的网络攻击，本书提出了网络安全预警防御机制。这里所谓的预警防御，是指在实时监控网络攻击的基础上，通过识别网络攻击意图，综合评估网络安全状态并预测其发展趋势，力争在攻击实施的早期阶段发出警报，并提前采取适当的手段予以防御，以尽可能在攻击未产生实质性危害时加以遏制，将损失降到最低。

网络攻击预警是一个具有前沿性的研究方向。早在 20 世纪 90 年代末，国外就开始了该方面的研究。如美国针对各信息基础设施提出的预警系统实现计划，英国 IAAC 组织开展的“Threat Assessment and Early Warning Methodologies for Information Assurance”项目等[4]。

经过多年努力，预警技术研究已经取得了很大进展。目前，针对大规模网络安全预警系统研究，急需解决以下两个方面问题[5]：①如何由局部发生的网络攻击预测其对全局的影响，做到从不同区域所发生的网络攻击来判断整体网络可能发生的入侵事件，并对其做出及时预警；②如何预测网络攻击方下一步可能采取的行动，有针对性地采取安全防御措施，及早启动应急方案。以上问题，主要涉及三项

关键技术，分别是网络攻击意图识别、网络安全态势感知和网络安全协同防护等。下面对这三项技术的研究现状加以分析。

1.2.1 网络攻击意图识别

1978 年，Schmidet 在文献[6]第一次提出规划识别问题（即本书的意图识别，Schmidet 不区分规划识别与意图识别），认为“规划识别”是通过观察人的行为去理解他的意图、信念和目标的过程，是心理学和人工智能的交叉问题。意图识别的研究最早应用于对自然语言理解[7,8]、故事理解[9,10]、语音翻译[11]等，随后逐渐应用到多智能体监测与协作[12,13]、动态交通监控[14]、冒险游戏[15]、网络入侵检测[16]、机器人[17,18]、军事[19,20]等。经过三十多年的发展，出现了很多模型和方法。如基于解释的意图识别方法、基于决策理论的意图识别方法、基于规划图分析的意图识别方法、基于概率推理的意图识别方法等。

在网络安全领域，多源信息融合领域的态势评估技术和人工智能领域的意图识别技术有强烈的应用需求和良好的发展前景，许多学者开始关注网络安全态势评估和网络攻击意图识别的研究。Bass[21]提出下一代的入侵检测系统：应用多传感器数据融合理论建立网络空间的态势感知的框架，通过推理识别攻击者身份、攻击速度、入侵行为、攻击意图和进行威胁分析等，进而感知网络空间的安全态势。文献[22]借鉴军事战场的意图识别方法开展了网络攻防对抗下的入侵意图识别和入侵策略的研究。攻击手段的灵活多变使得通过低层次的系统事件或网络事件分析入侵者的攻击策略变得非常困难，而高层次的意图识别能够提供独立于具体攻击手段的高水平的分析平台。在意图分析的层面上，入侵检测就变成使用各个异构的 IDS 协同工作去证实或者否定事先定义的各种意图假设。这两篇文献仅仅提出理论和概念的架构，没有提出具体的实现方法，更没有形成实用的原型系统。目前，国内外对网络攻击意图识别的研究才刚刚开始，还没有见到比较完整的理论、方法以及实用的系统。下面介绍与之类似或相关的主要研究。

1.2.1.1 借鉴其他领域的规划识别方法

Honeywell 实验室的 Geib 等[23]将人工智能领域的规划识别引入到网络安全领域中来，并指出网络安全领域中的规划识别与传统的规划识别不同，是一种对抗式的规划识别。因为攻击者总是采取欺骗、隐蔽等手段掩盖自己的行为和意图。该方法将主体所有的可能攻击行为作为扩展集，当攻击发生时，删除已经发生的行为，添加可能的攻击行为，构成新的扩展集。扩展集中概率最大的行为就是主体最可能的攻击规划。该方法能够利用观察到的数据推测攻击者的目标和正在执行的规划，但存在一些不足：很难构建完备的规划库；为了更新扩展集需要搜索主体所有可能的行为，可能引发搜索空间爆炸。文献[24]在规划识别基础上结合网络攻防对抗的特点提出了基于扩展目标规划图的网络攻击规划识别方法。该方法将观

察到的具体动作转化为抽象动作，根据抽象动作之间的关联识别背后蕴藏的攻击规划，这与将报警泛化为超报警的本质是相似的。文献[25]建立了入侵检测的规划识别模型，采用因果告警关联分析和贝叶斯推理网络实现规划识别，以找回因入侵检测自身的检测策略不足和网络覆盖范围脆弱性而丢失的关键告警，重构实际的攻击场景。这三项研究在人工智能领域中意图识别的经典方法基础上作了相应改进，提出了思路和理论框架。但是，这些研究主要还是对已经发生的攻击行为的识别和提炼上，对网络安全领域的复杂特点没有针对性，对不确定性的描述和推理、攻击者的意图（最终目标）识别以及威胁分析等的研究还没有开展。

1.2.1.2 基于攻击行为的报警关联、攻击场景构建

Cuppens 等[26]在 MIRADOR 项目中通过报警关联分析来提炼攻击者的入侵策略。对攻击行为的前提、后果进行建模，根据后续行为的前提与先前行为的后果是否匹配来对两个行为进行关联。当检测到攻击行为时，搜索满足匹配条件的攻击路径来构造攻击者的规划。当有多条攻击路径对应着不同的攻击目标时，选择最短的攻击路径对应的攻击目标作为攻击者的入侵意图。随着事件数量的增多，关联搜索空间急剧增大，不适合大规模的在线处理。而且，当攻击者的行为对应着多个攻击目标时，选择最短路径显然不能达到最佳的效果。Qin 等[27]将攻击树转化为因果网络，并关联孤立的攻击场景，利用专家知识给出因果网络的先验概率分布，推理攻击者的意图和后续的攻击行为。该方法需要先验知识来构建因果网络和条件概率。Ning 等[28]提出通过报警关联自动生成攻击策略的方法。攻击策略通过攻击策略图来描述，节点代表攻击行为，边代表攻击的时间顺序，边与节点的约束关系将攻击行为关联起来。该方法将一些形式不同但本质相同的报警泛化成超报警后再进行关联，增加了灵活性，提高了关联效率，并度量攻击策略间的相似性来发现攻击策略的本质，简化攻击策略分析。

文献[29]提出了基于入侵意图的复合攻击检测和预测算法。该算法在分析单步攻击目的的基础上，将复合攻击的各个步骤关联起来，完成复合攻击的入侵检测。文献[30]提出将报警抽象，在较高的层次上进行因果关联，利用时间着色 Petri 网来描述攻击状态的变迁。该方法能较好地检测和刻画复合攻击，具有较强的灵活性和容错性，并可利用已观察到的攻击与提前建好的攻击场景匹配来预测后续的攻击行为。类似的研究还有基于隐马尔科夫模型的攻击意图识别方法[31]、基于意图识别的报警信息关联处理模型[32]等。这些文献中提到的意图是指网络入侵者完成单步攻击的目的，是对单个行为的抽象和提炼，因此这些研究仍然属于报警关联和攻击场景构建的范畴，与本文的意图（攻击者的终极目标）识别有本质区别。

攻击图提供了一种描述攻击场景的可视化方法。通过构建攻击图来枚举攻击者所有可能的攻击行为，成为近年来研究的热点。对脆弱性利用进行分析和关联，

能够从模拟攻击的角度来推理和预测攻击者的入侵行为。该技术综合考虑网络拓扑结构、脆弱性信息、防火墙规则等信息，以攻击图的形式来对目标网络进行安全分析。文献[33]提出应用模型检测方法来自动生成攻击图。模型检测器通过发现违背安全策略的反例构造攻击图，每个反例都是一条可能的攻击路径。文献[34]应用攻击图的连接矩阵聚类技术来降低攻击图的复杂度，使其便于理解。文献[35]提出 MulVAL 框架，实现了基于策略的多主机、多步骤的脆弱性分析。网络的模型化表示以及攻击规则的简化，可以大大减少攻击图的生成时间。文献[36, 37]提出一种基于防火墙规则和脆弱性信息的攻击图生成工具 NetSPA。该工具能分析攻击者从网络中某台主机到达关键资产的可达性，在此基础上可以度量或采取措施确保目标网络的安全。文献[38]提出基于攻击路径分析的威胁评估模型T－MAP，能够根据单个脆弱性的利用难度、影响范围、可信度等多项属性来度量商用软件的安全性。通过不断地努力，克服了规模大、生成时间慢等早期研究出现的问题。但是，目前的研究大多都是静态的分析，不能根据实时的攻击行为和响应措施自适应地调整攻击图的生成与显示。而且不同的攻击路径由于难度、隐蔽度等存在差异，被利用的概率必然不同，对这种不确定性的研究目前还不充分。

1.2.2 网络安全态势感知

态势感知(Situation(al) Awareness，SA) 的概念最早来自于军事领域。军语中“态势”的含义是指交战双方的兵力部署在战场环境中呈现的“体态”与“阵势”。而所谓的“态势评估(Situation Assessment，SA)”、“态势感知”都是与战场态势相关的术语，严格说，它们的含义既有联系又有区别，其共同点是它们都会对军事指挥人员的作战决策产生影响，但各自强调的侧面又有所不同。态势评估是指对战场态势的综合评价，是将影响作战进程的多种因素综合为一种单一效能的评价目标，提供简洁明了的可理解的态势描述性术语“优势”、“均势”、“劣势”等供指挥决策者参考，属于评价过程；态势感知是指感知(perception)和发现对作战进程产生影响或将使战场态势发生转变的相关事件，属于认知(cognitive)过程[39]。本书中，不对这两个概念加以区别，均是指包含态势觉察、态势理解、态势预测三个阶段的完整的态势评判过程。

网络态势感知(Cyber Space Situational Awareness，CSA)的概念最早由 Bass 于 1999 年提出。所谓网络态势是指由各种网络设备运行状况、网络行为以及用户行为等因素所构成的整个网络的当前状态和变化趋势。值得注意的是，态势强调环境、动态性以及实体间的关系，是一种状态、一种趋势、一个整体和宏观的概念，任何单一的情况或状态都不能称其为态势[40]。

网络安全态势感知是网络态势感知的一个分支，是针对网络安全具体特点设计的模型和方法，它综合各方面的安全因素，从整体上动态反映网络的安全状态，

并对其发展趋势进行预测。

在安全威胁日趋严重的今天,对网络安全态势感知的研究具有非常现实的需要性。从文献发表情况看,目前的网络安全态势感知技术主要是根据单个或几个安全指标量化网络的安全状态,为用户理解当前的安全状态提供一定的参考依据。网络安全态势感知的研究主要包括评估模型和方法的研究、态势预测的研究和可视化研究三个方面。

1.2.2.1 模型和方法的研究

从文献发表情况看,绝大多数的研究集中于该方向,成果比较完善,趋于统一。如,文献[41]提出的层次化网络安全威胁态势定量评估模型能够直观地给出整个网络系统、主机和服务3个层次的安全威胁态势,使网络安全管理员能够及时了解系统安全动态,及时调整安全策略。但是该模型主要基于网络入侵检测系统的报警和网络带宽占有率,这些信息还不能全面反映攻击者的行为。文献[42]提出一种基于日志审计与性能修正算法的网络安全态势评估模型,针对网络安全性的各种关键因素进行建模,利用日志审计评估节点安全威胁,并通过性能修正算法计算节点安全态势,再利用节点服务信息计算网络安全态势。文献[43]提出一种基于弱点关联和安全需求的网络安全量化方法。该方法利用攻击图来计算各弱点被网络攻击者成功利用的概率,在此基础上,计算各弱点对主机可用性、保密性和完整性的影响。

1.2.2.2 态势预测的研究

态势预测的研究在近几年才渐渐引起人们的重视,成果逐渐增多,研究的目的在于如何通过不断修正预测模型以提高预测的精度。如,文献[44]提出的基于时间序列分析的态势预测算法,对由态势评估算法得到的过去和当前多个时段的网络安全态势值样本进行时间序列分析,从而实现对未来的网络安全趋势进行预测。文献[45]在充分考虑网络态势的流动性、突发性、周期性、非线性等特征的前提下,提出了网络态势预测的广义回归神经网络模型GRNNSF(generalized regression neural network model of networksituation forecast),详细论述了GRNNSF设计以及预测方法流程,并通过在真实网络数据上的实验对GRNNSF进行验证和比较。文献[46]则认为,安全态势序列蕴含了一系列复杂多变的随机趋势,突发性很强,不确定性很大,很难辨识和描述其规律,不是传统算法靠某个公式或函数就能表达及预测的,依据超长态势序列估计参数既很必要、也很困难,沿用现有的预测算法将难以避免与该领域特有问题的严重脱节。针对以上问题,他们提出了一种基于场景平移的预测方法,从录制的历史态势序列中查找相似迹象,衡量事发迹象与延续效应的联系强度,依据当前迹象推测某种效应重现的可能性,加权合成预测结果,另辅以进化算法,从形态及精度上计量预测偏差,通过逐步微调持续提升适应性。