国防科技著作精品译丛
网电安全系列

Springer

Cyber Situational Awareness Issues and Research

网络空间态势感知问题与研究

【美】Sushil Jajodia Peng Liu Vipin Swarup Cliff Wang 著

余健 游凌 樊龙飞 周德川 译

国防工业出版社
National Defense Industry Press

网络空间态势感知问题与研究

Cyber Situational Awareness Issues and Research

[美] Sushil Jajodia Peng Liu Vipin Swarup Cliff Wang 著

余健 游凌 樊龙飞 周德川 译

国防工业出版社
National Defense Industry Press

著作权合同登记　图字: 军 - 2013 - 047 号

图书在版编目（CIP）数据

网络空间态势感知问题与研究/（美）贾约迪亚（Jajodia, S.）等著;
余健等译. — 北京: 国防工业出版社, 2014. 7
（国防科技著作精品译丛. 网电空间安全系列）
书名原文: Cyber situational awareness:issues and research
ISBN 978-7-118-09578-4

Ⅰ. ①网… Ⅱ. ①贾… ②余… Ⅲ. ①互联网络—安全技术—研究
Ⅳ. ①TP393.408

中国版本图书馆CIP数据核字（2014）第 161923 号

Translation from English language edition:
Cyber Situational Awareness: *Issues and Research*
By Sushil Jajodia, Peng Liu, Vipin Swarup and Cliff Wang
Copyright © 2010 Springer US
Springer US is a part of Springer Science+Business Media
All Rights Reserved
本书简体中文版由 Springer US 国防工业出版社独家出版发行。
版权所有, 侵权必究。

网络空间态势感知问题与研究
[美] Sushil Jajodia　Peng Liu　Vipin Swarup　Cliff Wang　著
余健　游凌　樊龙飞　周德川　译

出版发行　国防工业出版社
地址邮编　北京市海淀区紫竹院南路 23 号　100048
经　　售　新华书店
印　　刷　北京嘉恒彩色印刷有限责任公司
开　　本　700 × 1000　1/16
印　　张　18¼
字　　数　302 千字
版 印 次　2014 年 7 月第 1 版第 1 次印刷
印　　数　1—2500 册
定　　价　86.00 元

(本书如有印装错误，我社负责调换)

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

翻译组名单

组　长：　余　健

副组长：　游　凌　樊龙飞　周德川

成　员：　张刚国　李洪轩　徐珍妮　杨　易　杨云龙
赵培焱　黄　宇　乔　良　贺英华　刘　建
曹卫权　闫方民　黄奇珊　张汇川　陆路希
王淮峰　燕继坤　周　密　石　芹　张　磊

译者序

进入 21 世纪以来, 随着信息技术和网络技术的飞速发展, 网络空间的重要性日益凸显, 网络空间已发展成为继陆、海、空、天之后的第 5 个域, 国家之间的网络对抗呈现出不断加剧之势, 网络空间战也演变成为一种新的作战样式, 并受到各国的重视。

网络空间态势感知是开展网络利用和网络攻防的基础和前提条件。它大致包括当前网络状态认知、恶意行为感知、恶意行为影响评估、态势追踪、因果分析和取证、态势感知信息 — 情报 — 决策的可靠性判断以及态势预测等 7 个方面的内容。

为推动我国的网络空间态势感知技术水平的提高, 加强网络空间能力建设, 我们通过广泛调研和筛选, 选取德国斯普林格出版社出版的《网络空间态势感知问题与研究》一书进行了翻译, 并提供给相关领导、专家和技术人员参考。

《网络空间态势感知问题与研究》出版于 2010 年, 由美国乔治梅森大学安全信息系统中心主任苏希尔 · 贾约迪亚 (Sushil Jajodia) 教授主编, 旨在介绍当代网络空间态势感知领域的发展情况, 为未来的研究工作提供指导。数十名来自网络安全、认知科学、决策科学等学科领域的专家或学者参与了本书的编写。本书共分成 11 章 (见目录部分), 系统介绍、分析和讨论了网络空间态势感知的涵义, 推理、决策与风险管理, 宏观网络态势感知, 企业级网络态势感知, 微观网络态势感知, 以及机器学习等问题。该书充分展现了国外对网络空间态势感知的研究成果, 具有很强的知识性、技术性和前沿性, 对于我国从事相关工作的人员了解和掌握网络空间态势感

试读结束，需要全本PDF请购买 www.ertongbook.com

知的新理论及方法, 开展网络态势感知技术研究, 提升网络态势感知能力具有重要的参考价值。

本书第 1 章由张刚国、李洪轩译, 第 2 章由徐珍妮、杨易译, 第 3 章由吉德川、杨云龙译, 第 4 章由周德川、赵培焱译, 第 5 章由黄宇、乔良译, 第 6 章由贺英华、刘建译, 第 7 章由贺英华、曹卫权译, 第 8 章由樊龙飞、闫方民译, 第 9 章由黄奇珊、张汇川译, 第 10 章由陆路希、王淮峰译, 第 11 章由燕继坤、周密、石芹译, 全书由游凌主审。由于我们水平有限, 不妥之处, 敬请指正!

译者

2014 年 6 月

前言

编写本书的动机

本书试图描绘网络空间态势感知技术的当前发展水平, 并为今后的研究确定方向。来自网络安全、认知科学和决策科学等学科的一组学术领头人详细阐述了研究界面临的基本挑战, 并鉴别了前景光明的解决途径。

今天, 每当发生网络安全事故的时候, 安全管理人员基本上都会提出 3 个问题: 发生了什么事? 为什么会发生这种事? 我应该做什么? 如何回答前两个问题构成了网络空间态势感知的核心。而最后一个问题是否有满意的答案, 则主要取决于一个企业的网络空间态势感知能力。

各种各样的计算机和网络安全研究课题 (尤其是一些系统安全课题) 都属于或是涉及到网络空间态势感知的范畴。然而, 一个企业的网络空间态势感知能力是十分有限的, 原因如下:

- 不准确和不完整的漏洞分析、入侵检测和取证分析;
- 缺乏监视某些微观系统/攻击行为的能力;
- 将信息转换、融合和提炼为网络情报的能力有限;
- 处理不确定性的能力有限;
- 现有的系统设计不太利于网络空间态势感知。

本书的目标是通过研究网络空间态势感知的整体性方法以及将现有的系统设计进化为能实现自我感知的新系统, 探索如何将企业的网络空间

态势感知能力提升到新的水平。本书的一个主要成果是给出了网络空间态势感知领域的一组科研目标和挑战。

关于本书

本书共有 11 章, 可以粗略地分为以下 6 个领域:

概述

- 网络空间态势感知: 网络防御态势感知。
- 网络空间态势感知概述。

推理与决策

- 基于识别主导决策的假设推理。
- 网络空间态势感知的不确定性与风险管理。

宏观网络空间态势感知

- 运用蜜网进行网络态势感知。
- 通过 WOMBAT 评估网络犯罪。

企业网络空间态势感知

- 拓扑漏洞分析。
- 网络空间态势感知的跨层损害评估。

微观网络空间态势感知

- 用于入侵分析的说明性框架。
- 自动化软件漏洞分析。

机器学习

- 高层次网络空间态势感知的机器学习方法。

鸣谢

我们非常感激所有对此书做出贡献的人们。感谢各位作者的付出。特别要感谢斯普林格出版社高级编辑苏珊 · 拉格斯托姆 - 菲弗和助理编辑沙龙 · 帕勒斯奇对此项目的大力支持。还要特别感谢宾夕法尼亚州立大学的张胜志, 他帮助把一些章节从 MS Word 格式转换为 LaTex 格式。

苏希尔 · 贾约迪亚

刘鹏

维平 · 斯瓦鲁普

克里夫 · 王

目录

试读结束，需要全本PDF请购买 www.ertongbook.com

第 1 章

网络空间态势感知: 网络防御态势感知

保罗 · 巴福特　马克 · 达希尔　托马斯 · G · 迪特里奇
马特 · 弗瑞德里克森　约翰 · 吉芬　苏希尔 · 贾约迪亚
索米什 · 杰哈　贾森 · 李　刘鹏　宁鹏　欧新明　宋道恩
劳拉 · 斯特瑞特　维平· 斯瓦鲁普　乔治 · 塔达
克里夫 · 王　约翰 · 伊恩

1.1 网络空间态势感知问题的范围

网络防御态势感知至少包括以下 7 个方面的内容:

(1) 了解当前状态, 也可称为态势认知。态势认知包括状态识别与确认。状态识别只是意识到有攻击正在发生, 而状态确认包括确认攻击类型、来源、属性和攻击目标等。态势认知不仅仅是入侵检测, 入侵检测只是其

保罗 · 巴福特, 威斯康星大学; 马克 · 达希尔, 赛门铁克公司; 托马斯 · G · 迪特里奇, 俄勒冈大学; 马特 · 弗瑞德里克森, 威斯康星大学; 约翰 · 吉芬, 佐治亚理工学院; 苏希尔 · 贾约迪亚, 乔治 · 梅森大学; 索米什 · 杰哈, 威斯康星大学; 贾森 · 李, 智能自动化有限公司; 刘鹏, 宾夕法尼亚大学; 宁鹏, 北卡罗来纳大学; 欧新明, 堪萨斯大学; 宋道恩, 加利福尼亚大学伯克利分校; 劳拉 · 斯特瑞特, SA 技术有限公司; 维平 · 斯瓦鲁普, MITRE 公司; 乔治 · 塔达, 美国空军研究实验室, 纽约州罗马市; 克里夫 · 王, 美国陆军研究局; 约翰 · 伊恩, 宾夕法尼亚大学。

苏希尔: 贾约迪亚等 (编辑),《网络空间态势感知, 信息安全技术的进展》第 46 卷, DOI10.1007/978-1-4419-0140-8-1, ©斯普林格科学与商业传媒有限责任公司, 2010。

试读结束，需要全本PDF请购买 www.ertongbook.com