网络空间安全前沿技术丛书

凡走过必留痕，凡寻找必有获，大数据时代无秘密……

[美] 马克·瑞恩 M. 塔拉比斯（Mark Ryan M. Talabis）
罗伯特·麦弗逊（Robert McPherson）
伊内兹·宫本（I. Miyamoto）
杰森 L. 马丁（Jason L. Martin）
著

王晓鹤　沈卢斌　译

信息安全分析学

大数据视角下安全的内核、模式和异常

清華大學出版社

网络空间安全前沿技术丛书

信息安全分析学

大数据视角下安全的内核、模式和异常

[美] 马克·瑞恩 M. 塔拉比斯（Mark Ryan M. Talabis）
罗伯特·麦弗逊（Robert McPherson）
伊内兹·宫本（I. Miyamoto）
杰森 L. 马丁（Jason L. Martin） 著

王晓鹤 沈卢斌 译

清華大學出版社
北京

图书在版编目(CIP)数据

信息安全分析学：大数据视角下安全的内核、模式和异常/(美)马克·瑞恩 M. 塔拉比斯(Mark Ryan M. Talabis)等著；王晓鹤，沈卢斌译. —北京：清华大学出版社，2019

(网络空间安全前沿技术丛书)

书名原文：Information Security Analytics：Finding Security Insights，Patterns，and Anomalies in Big Data

ISBN 978-7-302-50992-9

Ⅰ. ①信… Ⅱ. ①马… ②王… ③沈… Ⅲ. ①信息安全—系统安全分析 Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字(2018)第 191834 号

责任编辑：梁 颖
封面设计：常雪影
责任校对：时翠兰
责任印制：刘海龙

出版发行：清华大学出版社
网 址：http://www.tup.com.cn，http://www.wqbook.com
地 址：北京清华大学学研大厦 A 座 邮 编：100084
社 总 机：010-62770175 邮 购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 刷 者：北京富博印刷有限公司
装 订 者：北京市密云县京文制本装订厂
经 销：全国新华书店
开 本：190mm×235mm **印 张**：13 **字 数**：170 千字
版 次：2019 年 4 月第 1 版 **印 次**：2019 年 4 月第1次印刷
定 价：59.00 元

产品编号：073391-01

王晓鹤，现就职于爱立信通信有限公司任高级软件工程师。曾先后任职于中兴通讯公司和阿尔卡特朗讯公司，担任高级测试工程师、产品经理等职务，长期从事电信网络系统产品和数据网云平台产品的研发和测试工作。拥有德国乌尔姆大学信息和媒体专业理学硕士学位和东南大学通信工程学士学位。

沈卢斌，毕业于瑞典皇家理工学院（KTH）片上系统（SoC）设计专业。长期从事电信云计算平台的研发和系统安全的测试工作，是首批同时通过CCIE和HCIE认证的网络专家之一。对SDN安全、FPGA在工业互联网交换机中的设计以及基于FPGA的入侵检测系统有浓厚的兴趣和独到的见解。

译有《Google Hacking：渗透性测试者的利剑（原书第3版）》《信息安全分析学：大数据视角下安全的内核、模式和异常》《悄无声息的战场：无线网络威胁和移动安全隐私》和《防范互联网上的“野蛮人”：钓鱼检测、DDoS防御和网络攻防》等译著。

作者简介

- **Mark Ryan M. Talabis**
  担任Zvelo Inc.公司的首席安全威胁科学家，《信息安全风险评估工具包：通过Syngress的数据收集和数据分析进行实用评估》一书的合著者。

- **Robert McPherson**
  领导“美国财富100强”保险和金融服务公司的数据科学家团队。作为研究和分析团队的带领者，他拥有14年的领导经验（专门从事预测建模、仿真、计量经济分析和应用统计的工作）。

- **I. Miyamoto**
  担任政府机构的计算机调查员，拥有超过16年的计算机调查和取证经验，以及12年的情报分析经验。

- **Jason L. Martin**
  高级威胁检测技术领域的全球领导者FireEye Inc.公司的云业务副总裁，Shakacon安全大会的联合创始人，《信息安全风险评估工具包：通过Syngress的数据收集和数据分析进行实用评估》一书的合著者。

北京市版权局著作权合同登记号　图字：01-2017-5199
Information Security Analytics：Finding Security Insights，Patterns，and Anomalies in Big Data
Mark Ryan M. Talabis，Robert McPherson，Inez Miyamoto，Jason L. Martin
ISBN：9780128002070

信息安全分析学：大数据视角下安全的内核、模式和异常（王晓鹤，沈卢斌　译）
ISBN：9787302509929

注意

本书涉及领域的知识和实践标准在不断变化。新的研究和经验拓展我们的理解，因此须对研究方法、专业实践或医疗方法作出调整。从业者和研究人员必须始终依靠自身经验和知识来评估和使用本书中提到的所有信息、方法、化合物或本书中描述的实验。在使用这些信息或方法时，他们应注意自身和他人的安全，包括注意他们负有专业责任的当事人的安全。在法律允许的最大范围内，爱思唯尔、译文的原文作者、原文编辑及原文内容提供者均不对因产品责任、疏忽或其他人身或财产伤害及/或损失承担责任，亦不对由于使用或操作文中提到的方法、产品、说明或思想而导致的人身或财产伤害及/或损失承担责任。

本书献给

致力于

商用SD-WAN智能广域网平台应用开发的

华斧网络科技（AXESDN）公司

所有网络专家

译者序

信息安全本身的内涵非常丰富，有史以来就是伴随着人类文明社会不断运行和发展的议题。智慧的古人早就将信息安全看作关乎社稷存亡的重大问题，《周易·系辞上》中就有这样的论述，“故君子凡节天下，不可不周密之，苟能周密慎重，不露其芒角，使小人不得间而窥，则可免其过咎矣。”而在古今中外的军事斗争史上，不可胜数的战役胜败都能在敌对双方信息安全得失的问题上找到些许凭据，对信息安全的轻视和不当处理，轻则密泄事败，重则城破国灭。先秦时代使用的虎符，古希腊时代使用的斯巴达密码棒，都是人类先祖们对信息安全的重视和采取防范措施的经典案例。在科技迅猛发展的今天，尤其当前人类社会自 20 世纪进入以计算机和网络为代表的大信息时代以来，数据信息安全不但成为互联网这个看不见硝烟的战场上的无形主角，更随着网络日益融入人类日常生活及社会活动的方方面面而拥有了巨大的影响力。黑客或犯罪集团渴望并坚持不懈地尝试掌控和拥有这种力量以获取巨大利益的行动，也无时无刻不成为飘在我们每个公民、企业组织乃至国家天空上的乌云。这是一场持久的、敌暗我明的攻防战争。而令我感到会心的是，本书开篇立意的宗旨，恰恰很好地诠释并贯彻了

兵圣孙武早在两千五百多年前的战争巨著《孙子兵法》中就已经提出的“戒之于无形，防患于未然”的斗争战略：“无恃其不来，恃吾有以待之。无恃其不攻，恃吾有所不可攻也。”借助于计算机技术、统计学、可视化技术、仿真技术以及当下炙手可热的机器学习和大数据分析，网络信息犯罪的手法越来越隐蔽和先进，信息安全的防范手段也变得越来越多样和强大。然而万变不离其宗，抢先一步发现潜在性的破坏力量和风险，做到防患于未然并采取先发制人的措施将其消灭于襁褓之中，是本书的作者力图通过循序渐进的7章内容向我们讲解和传达，并期望成为我们能够掌握和运用以之对抗网络犯罪的有力铁拳。

我们很高兴能够发现《信息安全分析学》这样一本针对网络信息安全领域具有如此实用性和可操作性，同时也不失一定广度和深度的技术书籍。更高兴能够在清华大学出版社的鼎力支持下将其翻译出版，而让广大的专业技术人员及研究者和我们一起分享和探究这本好书。如果你能从本书中学习和掌握些什么并将之付诸工作和学习的实战中取得胜果，这将是对我们翻译工作的最大褒扬和肯定。

由于译者水平所限，书中难免存在遗漏或有失准确之处，欢迎广大读者不吝指正。另外在本书的翻译过程中，我们得到了清华大学出版社电子信息事业部梁颖主任的大力帮助，在此我们表示由衷的感谢。

译　者

2018年6月于上海

题　献

谨以此书献给 Joanne Robles，Gilbert Talabis，Hedy Talabis，Iquit Talabis 和 Herbert Talabis。

Ryan

我想将本书献给我的妻子 Sandy 和我的儿子们——Scott，Chris，Jon 和 Sean，没有他们的支持和鼓励我也不会参与这个项目。我也欠我的爱犬 Lucky 一个人情，它总是知道该在何时提醒我需要休息，那时它都会把鼻子放在我的手下面并将其从键盘上顶开。

Robert

谨以此书献给我的朋友、家人、导师，以及所有不知疲倦地致力于系统安全工作的安全专业技术人员。

I. Miyamoto

前　言

信息安全是一个具有挑战性的领域，伴随着众多未解决的难题以及如何解决这些难题的诸多争论。与诸如物理学、天文学以及类似科学的其他领域相比较，在发现信息安全问题严重影响我们生活的世界之前，我们没有机会能让信息安全领域屈服于那些谨慎的理论分析。互联网就是安全研究的试验场，而且为了保持适当的防卫以对抗在这个活跃的虚拟有机体上进行的攻击性研究，这会是一场持续的战斗。有大量关于信息安全卷入真实间谍情报技术的行业炒作，尤其是关于“分析论”和“大数据”的炒作，本书上架正是为了努力启发读者，当运用数据科学来加强安全研究时，能够获得什么样的真正价值。这本内容丰富的图书并不意味着能被普通读者迅速阅读和理解，相反，对于研究人员和从事安全领域工作的读者，本书恰恰值得他们钻研并运用于工作，力求以实用和先发制人的方式去运用数据科学来解决日益变得困难的信息安全问题。

Talabis，McPherson，Miyamoto 和 Martin 的工作在本书中完美融合并通过本书传递了如此迷人的知识，即向读者展示了分析论对影响全球企业和组织的各种问题的适用性。记得 2010 年当我仍在 Damballa 工作时，我所在

的研究部一直在探索数据科学、机器学习、统计学、相关性和分析论等领域。那是一段激动人心的时期，R 语言在当时越来越流行，暗示着信息安全的新篇章即将开始。它确实到来了，但是很多营销流行语也随之被创造，所以现在我们有“安全分析论”“大数据”和“威胁情报”，当然“网络”对任何人都没有真正的意义，直到现在。

《信息安全分析学》是我读过的，而且直接可以将从书中学到的知识运用到团队工作中的少数几本技术书籍之一。本书还介绍了一些更加主动的见解，也就是通过致力于信息安全领域的纯粹研究方面来解决这些问题。这比我们目前依靠诸如 SIEM、威胁馈送和基本相关性及分析论等操作性的答案要好得多。我的工作涉及 Cyber Counterintelligence 与位列全球四大咨询公司之首的公司的研究工作，而且数据科学和纯安全性研究的价值正在被发掘和认可。但就本书而论，我丝毫不怀疑在这些章节中提供的知识将把我的团队和整个公司提升到另一个层面。就谈到这里吧，我非常荣幸能够说，好好享受这本书吧！

Lance James
Head of Cyber Intelligence
Deloitte & Touche LLP

致　谢

首先，我最要感谢我的合作者 Robert McPherson 和 I. Miyamoto 在本书写作之前、期间和之后的支持。我要感谢我的老板和朋友 Jason Martin，感谢他全部的指导和智慧。我还要感谢 Howard VandeVaarst 的全力支持和鼓励。最后，特别感谢 Zvelo 公司的所有同仁欢迎我加入他们的家庭。

Ryan

我想感谢 Ryan Talabis 在哈佛大学的比萨派对上邀请我参与这个项目。我也想感谢 I. Miyamoto 帮助我能保持在正确的写作轨道上并提供有价值的反馈。此外我发现 Pavan Kristipati 和 D. Kaye 的技术专长以及编辑建议对我非常有帮助，我非常感谢他们的支持。

Robert

我非常感谢 Ryan 和 Bob 的无条件支持以及提供给我参与这个项目的机会。特别应该感谢我们技术审核人员的超乎寻常的鼎力相助来改进我们的工作，还要特别感谢 Elsevier 团队给予的帮助支持和耐心。

I. Miyamoto

全体作者由衷感谢 James Ochmann 和 D. Kaye 帮助准备了手稿。

专门从事预测建模、仿真、计量经济分析和应用统计的工作。Robert 与一组研究人员合作，利用仿真和大数据方法对涉及价值数百万保险政策的灾难影响进行建模，模拟长达 10 万年的飓风、地震和大火，以及严冬和夏季风暴，被保险财产的价值超过 2 万亿美元。他利用预测建模和先进的统计方法来开发自动化异常值检测方法，构建自动化承保模型、执行产品和客户细分分析，并设计与竞争对手的对战游戏模拟。他拥有哈佛大学进修教育学院信息管理硕士学位。

I. Miyamoto 目前担任政府机构的计算机调查员，拥有超过 16 年的计算机调查和取证经验，以及 12 年的情报分析经验。正在进修系统工程博士学位，并拥有以下学位：软件工程学士学位、国家安全和战略研究硕士学位、战略情报硕士学位以及教育学博士学位。

Jason L. Martin 高级威胁检测技术领域的全球领导者 FireEye Inc. 公司的云业务副总裁。在加入 FireEye 公司之前曾担任 Secure DNA 公司（被 FireEye 收购）的总裁兼首席执行官，该公司为泛亚太和美国大陆的公司提供创新的安全产品和解决方案。客户包括财富 1000 强公司、全球政府机构、州和地方政府以及各种规模的私人机构。他在信息安全方面拥有超过 15 年的经验，是一位出版作家和演讲者，也是 Shakacon 安全大会的联合创始人。

目　录