O'REILLY®

网络安全科学本质论

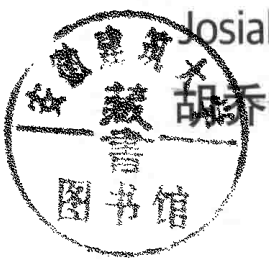
Essential Cybersecurity Science

Josiah Dykstra 著
胡乔林 陈新 译

出版社

网络安全科学本质论

Josiah Dykstra 著
胡乔林 陈新 译



Beijing · Boston · Farnham · Sebastopol · Tokyo O'REILLY®

O'Reilly Media, Inc. 授权中国电力出版社出版

中国电力出版社

图书在版编目（CIP）数据

网络安全科学本质论 / (美) /乔西亚·戴克斯特拉（Josiah Dykstra）著；胡乔林，陈新译. —北京：中国电力出版社，2018.9

书名原文：Essential Cybersecurity Science

ISBN 978-7-5198-2355-9

I. ①网… II. ①乔… ②胡… ③陈… III. ①计算机网络－网络安全 IV. ①TP393.08

中国版本图书馆CIP数据核字(2018)第195503号

北京市版权局著作权合同登记 图字：01-2018-3070号

出版发行：中国电力出版社
地　址：北京市东城区北京站西街19号（邮政编码100005）
网　址：http://www.cepp.sgcc.com.cn
责任编辑：刘 炽（liuchi1030@163.com）
责任校对：黄 蓓，王海南
装帧设计：Ellie Volkhausen，张 健
责任印制：杨晓东

印　刷：北京天宇星印刷厂
版　次：2018年9月第一版
印　次：2018年9月北京第一次印刷
开　本：750毫米×980毫米 16开本
印　张：12
字　数：221千字
印　数：0001—3000册
定　价：48.00元

O'Reilly Media, Inc.介绍

O'Reilly Media通过图书、杂志、在线服务、调查研究和会议等方式传播创新知识。自1978年开始，O'Reilly一直都是前沿发展的见证者和推动者。超级极客们正在开创着未来，而我们关注真正重要的技术趋势——通过放大那些“细微的信号”来刺激社会对新科技的应用。作为技术社区中活跃的参与者，O'Reilly的发展充满了对创新的倡导、创造和发扬光大。

O'Reilly为软件开发人员带来革命性的“动物书”；创建第一个商业网站（GNN）；组织了影响深远的开放源代码峰会，以至于开源软件运动以此命名；创立了Make杂志，从而成为DIY革命的主要先锋；公司一如既往地通过多种形式缔结信息与人的纽带。O'Reilly的会议和峰会集聚了众多超级极客和高瞻远瞩的商业领袖，共同描绘出开创新产业的革命性思想。作为技术人士获取信息的选择，O'Reilly现在还将先锋专家的知识传递给普通的计算机用户。无论是通过书籍出版，在线服务或者面授课程，每一项O'Reilly的产品都反映了公司不可动摇的理念——信息是激发创新的力量。

业界评论

“O'Reilly Radar博客有口皆碑。”

——Wired

“O'Reilly凭借一系列（真希望当初我也想到了）非凡想法建立了数百万美元的业务。”

——Business 2.0

“O'Reilly Conference是聚集关键思想领袖的绝对典范。”

——CRN

“一本O'Reilly的书就代表一个有用、有前途、需要学习的主题。”

——Irish Times

“Tim是位特立独行的商人，他不光放眼于最长远、最广阔的视野并且切实地按照Yogi Berra的建议去做了：‘如果你在路上遇到岔路口，走小路（岔路）。’回顾过去Tim似乎每一次都选择了小路，而且有几次都是一闪即逝的机会，尽管大路也不错。”

——Linux Journal

目录

前言

本书的读者对象

科学适用网络安全的许多领域，本书的目标读者广泛而多样。这本书特别适合那些正在构建和评估网络安全硬件和软件解决方案的开发人员、工程师和企业家。其中，网络安全的从业人员（如电子取证人员、恶意软件分析人员和其他网络安全专家）的日常工作就是使用、构建和测试新工具。有些人具有编程经验，而另一些人具有各种安全工具的工作经验（包括用于取证的 Wireshark，用于网络分析的 Wireshark，用于逆向工程的 IDA Pro 等）。科学方法可以应用于所有这些领域。网络安全科学可以应用于日常问题，包括：

- 测试最新智能手机游戏中的漏洞。
- 在给定预算的情况下保护公司安全选择。
- 让人们相信你的新安全产品比竞争对手更好。
- 平衡入侵检测的准确性和性能。

本书核心受众是在该领域工作了 5~10 年的信息安全专业人员，他们正在成为其技术和领域的专家，在日常生活中没有接受过科学研究方面的正式培训或接触过科学调查，他们希望学习一种补充和改进其工作的新方法。我希望当你放下这本书后，知道如何对你的日常工具和程序上进行科学实验，并且知道在进行这些实验之后，你已经更安全、更准确、更有效地完成了你的工作。

这本书的目的不是要把你变成一个科学家，但它会向你介绍科学思维的规律。对于那些刚入门的人，包括网络安全专业的学生，本书将帮助你了解适用网络安全的科学方法，以及如何在新专业中进行科学实验。对于参与网络安全的非开发人员（例如使用、评估、购买和推荐公司安全解决方案的 IT 安全管理员），本书将帮助你进行实践实验，并解释其他人的科学主张。

本书内容

第1 ~ 3 章包含了有关科学方法的一般信息，因为它适用网络安全的许多领域。涵盖了科学的基本原理、网络安全对科学的需求以及科学研究的方法。第 1 章阐述了科学方法和科学对网络安全的重要性。第 2 章讨论了进行网络安全实验所需的先决条件，从提出好的问题到将结果付诸实施。它还包括一个核对表，以帮助你构建自己的实验。第 3 章包括实验的实践性细节，包括测试环境和开放数据集。

其余章节将组织成独立的特定领域的主题。你可以单独阅读它们，尽管这些章节中的新科学主题和技术适用于其他领域。这些章节探讨了如何将科学方法应用于特定主题和各领域的挑战。每一个专题章节都概述了该领域的科学研究、该领域科学实验的一个指导性实例、分析方法的介绍（可应用其他领域），以及贯穿科学方法应用与该领域的一个简单入门性实验的实践实例。

- 第 4 章介绍软件保障的网络安全科学，包括模糊模型和对手模型。
- 第 5 章介绍入侵检测和事件响应，并介绍错误率（假阳性和假阴性）和性能 / 可扩展性 / 压力测试。
- 第 6 章侧重于科学在网络态势感知中的应用，特别是使用机器学习和大数据。
- 第 7 章介绍密码学以及可证实的安全网络安全的益处和局限性。
- 第 8 章涉及数字取证，包括科学可再现性和可重复性。

- 第 9 章介绍了与恶意软件分析相关的博弈论和恶意软件族。
- 第 10 章讨论了使用安全工程构建和评估可靠系统。
- 第 11 章介绍了人机交互和安全可用性的经验性实验。
- 第 12 章包括安全可视化实验评估技术。

附录 A 提供了一些关于评估科学声明的额外信息，尤其是来自供应商的科学声明，以及人们如何被真实或虚假科学误导、操纵或欺骗。还有一个问题清单，你可以使用它与销售人员、研究人员和产品开发人员探讨他们使用的方法。

本书约定

本书使用如下排版约定：

斜体 (italic)

表示新术语、URL、email 地址、文件名、文件扩展名等。

等宽字体（constant width）

表示程序列表，同时在段落中引用的程序元素（例如变量、函数名、数据库、数据类型、环境变量、声明和关键字等）也用该格式表示。

等宽黑体（**constant width bold**）

表示需要用户逐字符键入的命令或其他文本。

等宽斜体（*constant width italic*）

表示应该以用户提供的值或根据上下文决定的值进行替换的文本。

表示一个提示或者建议。

表示一般性说明。

表示警告或者注意要点。

Safari Book Online

Safari Book Online（*www.Safaribookonline.com*）是一个按需定制的数字化图书馆，它发布来自全世界技术和业务上最顶尖的作者的专业内容，包括书籍和视频。

技术专业人员、软件开发者、网页设计者和商业创新专业人员都可以使用Safari Book Online来作为研究问题、解决、学习和认证培训的主要资源。

Safari Book Online为组织者、政府机构和个人提供了各种价格范围的资源。订阅者可以通过一个统一的可搜索数据库访问成千上万的书籍、培训视频和预出版的手稿，提供资源的出版社包括O'Reilly Media、Prentice Hall Professional、Addison-Wesley Professional、Microsoft Press、Sams、Que、Peachpit Press、Focal Press、Cisco Press、John Wiley & Sons、Syngress、Morgan Kaufmann、IBM Redbooks、Packt、Adobe Press、FT Press、Apress、Manning、New Riders、McGraw-Hill、Jones & Bartlett、Course Technology等。如需更多关于Safari Book Online的信息，请访问我们的网站。

如何联系我们

请将关于本书的意见和问题发送给出版社：

美国：

O'Reilly Media，Inc.
1005 Gravenstein Highway North

Sebastopol，CA 95472

中国：

北京市西城区西直门南大街2号成铭大厦C座807室（100035）
奥莱利技术咨询（北京）有限公司

我们为本书提供了网页，该网页上面列出了勘误表、范例和任何其他附加的信息。你可以访问如下网址获得：*http://bit.ly/essential-cybersecurity-science*。

要询问技术问题或对本书提出建议，请发送电子邮件至：*bookquestions@oreilly.com*。

关于我们的书籍、课程、会议和新闻的更多信息，请参阅我们的网站：

http://www.oreilly.com
http://www.oreilly.com.cn

我们的 Facebook：*http://facebook.com/oreilly*。

我们的 Twitter：*http://twitter.com/oreillymedia*。

我们的 YouTube：*http://www.youtube.com/oreillymedia*。

免责声明

这本书表达的观点仅限于作者的观点。以商品名、商标、制造商或其他方式提及任何特定商业产品、工艺或服务，并不构成或暗示得到美国政府或国防部的认可、推荐或支持。

致谢

衷心感谢 Rachel Roumeliotis、Heather Scherer、Nan Barber 和 O'Reilly 的整个团队帮助我完成编辑和出版过程。感谢才华横溢和诚实的技术评论家 ichael

Collins 和 Matt Georgy，他们改进了本书的许多方面。感谢我的朋友和同事们对这个项目提供的反馈和支持：Janelle Weidner Romano、Tim Leschke、Celeste Lyn Paul、Greg Shannon、Brian Sherlock、Chris Toombs、Tom Walcott 和 Cathy Wu。还要感谢过去几年在网络安全科学大会、会议和研讨会上与我互动的朋友、同事和陌生人，特别是 LASER、CSET 和 HoTSoS。这些对话有助于影响和贡献本书的许多想法。最重要的是，感谢我的妻子 Alicia 在这个项目和所有事情中的爱和鼓励。

第 1 章

网络安全科学简介

本章将介绍网络安全科学的概念及其重要性、科学方法、网络安全理论与实践的关系，以及与科学有关的高级主题，包括人的因素和度量标准。

无论你是学生、软件开发人员、电子取证人员、网络管理员，或者在提供网络安全方面扮演任何其他角色，本书都将向你介绍有效网络安全的相关科学原则和灵活方法。本书关注的是科学在现实世界中对你提供网络安全的作用。你将学习到如何自己通过进行实验来评估安全保证。

让我列举一些理由，来说明为什么花费这么多精力在网络安全学科是值得的。

- **科学受到尊重**。大多数人认为科学探索和科学成果是有价值的。广告商总是喜欢它，即使科学是荒谬的或者是虚构的。如果你表现出具备良好的科学素养，人们会尊重你和你在网络安全方面的工作。一份报告说："在过去的几年里，人们将科学原理推广并应用于信息安全的想法有着浓厚的兴趣。" 科学研究有助于让听众相信成果的价值[注 1]。

- **科学很性感**。除了尊重之外，许多非科学家希望了解他们所仰慕的领域，并成为其中的一部分。科学曾经被认为是枯燥、无聊和极客，现在却成了一件令人钦佩的事情，越来越多的人希望被认同。

- **科学激起好奇心**。信息安全专业人士的好奇心很强。他们提出了很好的问题，并渴望得到信息，数据科学越来越受到重视就证明了这一点。科学是

注 1：Barriers to the Science of Security(*http://nsf.gov/events/event_summ.jsp?cntn_id=123377*)。

信息的载体，答案会激发更多的问题。科学探究带来了对网络安全领域更深刻的认识。

- **科学创造并改进产品**。在商业领域，市场推动网络安全。科学知识可以改进现有产品并导致突破性的创新和应用。对于信息安全决策者而言，科学方法可以使产品评估变得可靠和高效。

- **科学促进知识**。科学是人类挖掘世界新知识的主要方式之一。科学参与者有机会为人类理解自身做出贡献，并推动最先进的技术发展。特别是在网络安全方面，科学将有助于证明实践和有效的技术，使我们远离今天网络安全实践中的“民间智慧”。

科学实验和调查揭示了在优化和创建更安全的网络解决方案方面存在机会。例如，数学本身可以帮助密码学家确定如何设计更安全的加密算法，但数学并不能控制如何设计有用的网络映射可视化的过程。可视化需要实验和可重复的用户体验研究。在这种情况下的验证更像是判定设计选择的依据。 在用户环境下，NetFlow的最佳采样率是多少？试图回答这个问题，并最大限度地提高答案的有效性是一项科学努力。此外，你可以从别人过去的所作所为中吸取经验。

什么是网络安全科学

网络安全科学是理解、发展和实践网络安全的重要方面。网络安全是一个很广泛的类别，涵盖了用于保护计算机网络、计算机和数据免受伤害的技术和实践。工业界、学术界和政府的所有人都使用正式和非正式的科学来创建和扩展网络安全知识。作为一门学科，网络安全领域需要真实的实践知识来探索和推理我们构建或部署安全控制的“方式和原因”。

本文中谈论到的将科学和科学方法应用于网络安全，指的是利用关于网络安全的知识体系(科学)和一套特定的技术对照现实经验来检验假设(科学方法)。

获取知识的几种途径

科学调查不是获取知识的唯一途径。在非科学方法还包括常识、直觉和演绎。

常识描述大多数人共同的知识，通常与人类的经历有关。直觉是没有意识推理的知识获取。演绎法使用给定的前提来得出结论（例如，所有的人都终有一死，爱因斯坦是一个人，因此爱因斯坦也终有一死）。数学是演绎的，因为公理在没有被测试的情况下被假定为真。

Walter Vincenti 在他的著作《What Engineers Know and How They Know It》中提出了六类可以用于网络安全的工程知识：

- 基本的设计理念。
- 标准和规格。
- 理论工具。
- 定量数据。
- 实践考虑。
- 设计手段。

另一种天真但令人悲哀的推动网络安全科学的方法是未经了解和检验的猜测。我们猜测用户希望工具做什么。假想购买什么以及如何部署网络安全解决方案。猜测无法了解情况也是无效的，虽然它可能看起来有助于提高安全性，但它很难防御，往往失败得很惨。

不幸的是，科学因为憋闷和寒冷而著称，只有身穿白色实验室外褂的人才会对此感到兴奋。作为网络安全从业者，可以把科学看做一种探索你的好奇心的方法，一个发现意想不到的东西的机会，以及一个改进你工作的工具。

你每天都可以从网络安全人员所做的实验和科学调查中受益。举几个例子：