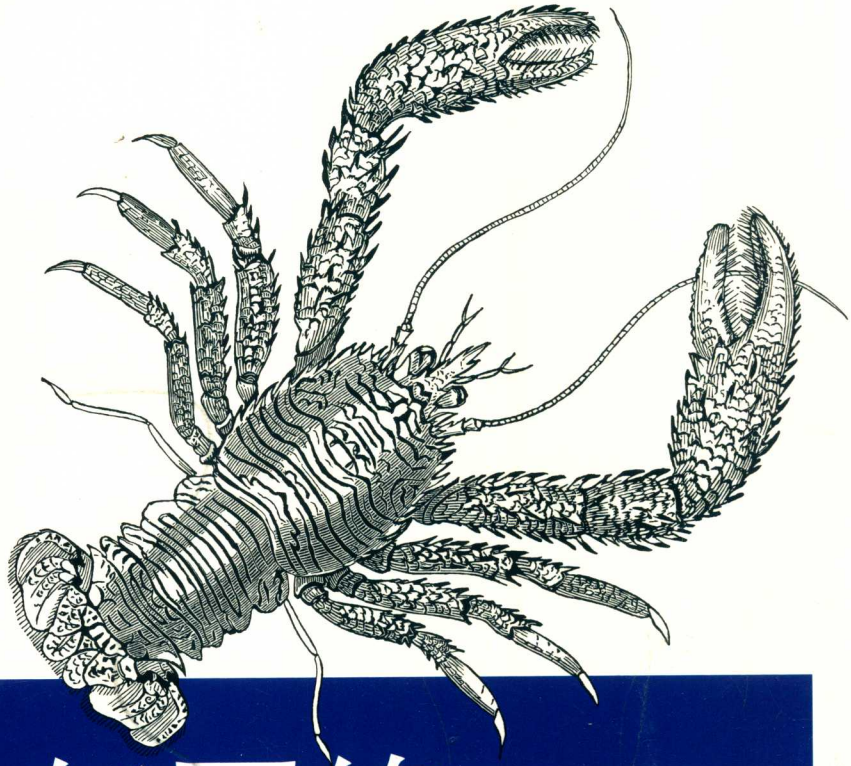
O'REILLY®

异步图书
www.epubit.com.cn



零信任网络

在不可信网络中构建安全系统

Zero Trust Networks

[美] 埃文·吉尔曼　道格·巴斯 著
奇安信身份安全实验室 译

中国工信出版集团　人民邮电出版社
POSTS & TELECOM PRESS

零信任网络

在不可信网络中构建安全系统

[美] 埃文·吉尔曼　道格·巴斯　著

奇安信身份安全实验室　译

Beijing • Boston • Farnham • Sebastopol • Tokyo

O'REILLY®

, Inc.授权人民邮电出版社出版

人民邮电出版社

北京

图书在版编目（CIP）数据

零信任网络 : 在不可信网络中构建安全系统 / (美)埃文·吉尔曼 (Evan Gilman)，(美) 道格·巴斯 (Doug Barth) 著 ; 奇安信身份安全实验室译. -- 北京 : 人民邮电出版社, 2019.8
ISBN 978-7-115-51002-0

Ⅰ. ①零… Ⅱ. ①埃… ②道… ③奇… 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(2019)第053188号

版权声明

◆ 著　[美] 埃文·吉尔曼（Evan Gilman）
[美] 道格·巴斯（Doug Barth）
译　奇安信身份安全实验室
责任编辑　陈聪聪
责任印制　焦志炜

◆ 人民邮电出版社出版发行　北京市丰台区成寿寺路 11 号
邮编　100164　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京鑫正大印刷有限公司印刷

◆ 开本：800×1000　1/16
印张：13.75
字数：252 千字　2019 年 8 月第 1 版
印数：1－5 000 册　2019 年 8 月北京第 1 次印刷

著作权合同登记号　图字：01-2018-7760 号

定价：59.00 元

读者服务热线：(010)81055410　印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京东工商广登字 20170147 号

内 容 提 要

本书分为 10 章，从介绍零信任的基本概念开始，描述了管理信任，网络代理，授权，建立设备信任、用户信任、应用信任以及流量信任，零信任网络的实现和攻击者视图等内容。本书主要展示了零信任如何让读者专注于构建强大的身份认证、授权和加密，同时提供分区访问和更好的操作敏捷性。通过阅读本书，读者将了解零信任网络的架构，包括如何使用当前可用的技术构建一个架构。

本书适合网络工程师、安全工程师、CTO 以及对零信任技术感兴趣的读者阅读。

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。O'Reilly将先锋专家的知识传递给普通的计算机用户，供技术人士获取信息。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

译者简介

奇安信身份安全实验室是奇安信集团下属的专注于“零信任身份安全架构”研究的专业实验室。该团队以“零信任安全，新身份边界”为技术思想，探索“企业物理边界正在瓦解、传统边界防护措施正在失效”这一时代背景下的新型安全体系架构，推出“以身份为中心、业务安全访问、持续信任评估、动态访问控制”为核心的奇安信天鉴零信任身份安全解决方案。该团队结合行业现状，大力投入对零信任安全架构的研究和产品标准化，积极推动“零信任身份安全架构”在业界的落地实践，其方案已经在部委、央企等得到广泛的落地实施，得到市场和业界的高度认可。同时，为帮助广大读者和技术爱好者更好地理解零信任安全架构及技术体系，奇安信身份安全实验室同步在线上成立零信任安全社区 （微信 ID：izerotrust），将定期分享和推送“零信任身份安全架构”在业界的研究和落地实践，欢迎广大读者和业界人士关注。

“零信任安全社区”公众号二维码

译者序

零信任（或零信任网络、零信任模型等）这个概念最早是由 John Kindervag 于 2010 年提出的，他当时是 Forrester 的分析师。John Kindervag 非常敏锐地发现传统的基于边界的网络安全架构存在缺陷，通常被认为“可信”的内部网络充满威胁，“信任”被过度滥用，并指出“信任是安全的致命弱点”。因此，他创造出了零信任（Zero Trust）这个概念。“从来不信任，始终在校验”（Never Trust，Always Verify）是零信任的核心思想。

传统的网络安全架构基于网络边界防护。企业构建网络安全体系时，首先把网络划分为外网、内网和 DMZ 区等不同的安全区域，然后在网络边界上通过部署防火墙、WAF 和 IPS 等网络安全技术手段进行重重防护，构筑企业业务的数字护城河。这种网络安全架构假设或默认了内网比外网更安全，在某种程度上预设了对内网中的人、设备、系统和应用的信任，从而忽视内网安全措施的加强。美国 Verizon 公司的《2017 年数据泄露调查报告》指出，造成企业数据泄露的原因主要有两类：一是外部攻击，二是内部威胁。随着网络攻防技术的发展，新型的网络攻击手段层出不穷，攻击者面对层层设防的网络边界，往往会放弃代价高昂的强攻手段，转而针对企业内部网络中的计算机，采用钓鱼邮件、水坑攻击等方法渗透到企业网络内部，轻松绕过网络边界安全防护措施。由于人们往往认为内网是可信任的，因此攻击者一旦突破企业的网络安全边界进入内网，就会如入无人之境。此外，企业员工、外包人员等内部用户通常拥有特定业务和数据的合法访问权限，一旦出现凭证丢失、权限滥用或恶意非授权访问等问题，同样会导致企业的数据泄露。

基于这样的认知，零信任针对传统边界安全架构思想重新进行了评估和审视，并对安全架构思路给出了新的建议：默认情况下不应该信任网络内部和外部的任何人、设备、系统和应用，而是应该基于认证和授权重构访问控制的信任基础，并且这种授权和信任不是静态的，它需要基于对访问主体的风险度量进行动态调整。

零信任对网络安全架构进行了范式上的颠覆，引导安全体系架构从网络中心化走向身份中心化，其本质诉求是以身份为中心进行细粒度的自适应访问控制。零信任所依赖的身份认证与访问控制能力通常由身份与访问管理系统（IAM）提供，现代身份管理技术是零信任安全的技术根基，因此，从技术方案层面来看，零信任是借助

现代身份管理技术实现对人、设备、系统和应用的全面、动态、智能的访问控制。

客观地说，John Kindervag 提出零信任架构的开始几年，这一理念并没有获得网络安全行业的普遍关注，只是在一些社区有着小范围的讨论和实践，本书的作者 Evan Gilman 和 Doug Barth 就是早期实践者之一。然而，2015 年前后，情况发生了明显的变化。层出不穷的高级威胁和内部风险，以及监管机构对企业网络安全的监督力度逐渐加强，使得零信任架构变革的外部驱动力越来越强。随着企业数字化转型的逐渐深入，以云计算、微服务、大数据、移动计算为代表的新一代信息化建设浪潮愈演愈烈，IT 基础设施的技术架构发生了剧烈的变革，导致传统的内外网络边界变得模糊，很难找到物理上的网络安全边界，企业自然无法基于传统的边界安全架构理念构筑安全基础设施。安全架构如果不能随需应变，自然会成为木桶最短的那块木板，零信任架构变革的内生驱动力也在持续加强。

2017 年，Google 对外宣布其基于零信任架构实践的新一代企业网络安全架构——BeyondCorp 项目成功完成，为零信任在大型、新型企业网络的实践提供了参考架构。这一最佳实践成为零信任理念的助推剂，各大安全厂商、分析机构和大型企业快速跟进，对零信任的推广和宣传也持续升温，在 RSAC 2019 展会上达到高潮，零信任俨然成为网络安全界的新宠。

当然，任何一种新生事物都难免受到人们的质疑，零信任架构也不例外。在过去一年多时间推广和实践零信任的过程中，我们遇到最多的质疑是，零信任听起来并没有什么新技术，是不是“新瓶装旧酒”？的确，零信任是一种全新的安全架构，但其核心组件基于身份与访问管理技术、终端设备环境风险评估技术、基于属性的访问控制模型、基于机器学习的身份分析技术等构建，听上去并没有太多激动人心的新技术。并且，零信任的最佳实践反倒是推荐使用现有的成熟技术，根据具体的应用场景，按照全新的逻辑进行组合，就能起到完全不同的安全效果。

我们认为零信任的创新和价值恰恰不在于具体的组件技术本身，而在于架构理念和安全逻辑层面。零信任架构与传统的边界安全架构、传统的安全防护理念最大的不同之处在于以下几点。第一，在网络安全边界瓦解、攻击面难以穷尽的情形下，与传统的安全理念不同，零信任架构引导人们更加关注“保护面”而不是“攻击面”。首先识别需要重点保护的资源对象，然后穷举分析该资源对象的访问路径，最后采用恰当的技术手段做好每条路径的访问控制措施。第二，零信任架构认为网络是不可信任的，因此不再寄希望于在传统的网络层面增强防护措施，而是把防护措施建立在应用层面，构建从访问主体到客体之间端到端的、最小授权的业务应用动态访问控制机制，极大地收缩了攻击面；采用智能身份分析技术，提升了内外部攻击和身份欺诈的发现和响应能力。第三，零信任架构在实践机制上拥抱灰度哲学，以安

全与易用平衡的持续认证改进固化的一次性强认证，以基于风险和信任持续度量的动态授权替代简单的二值判定静态授权，以开放智能的身份治理优化封闭僵化的身份管理。因此，灰度哲学是零信任安全的内生逻辑，也是零信任安全实践的指导原则。

零信任是一种全新的安全理念，它并不是严格定义的技术术语，这个概念的内涵和外延仍然处于变化之中。我们也不认为本书是一本零信任的教科书或者“圣经”，本书作者为我们揭示了零信任的基本概念和体系架构，并且通过实例介绍了如何利用现有的技术逐步构建一个零信任网络。我们希望通过翻译成中文的方式，可以把零信任的理念系统完整地介绍给国内的网络安全业界同仁，供大家讨论、实践和探索，甚至批判。希望能够通过这种方式，让更多的人理解和实践零信任理念，推动企业网络安全架构的转型和变革，为云计算和大数据时代的业务应用及数据保驾护航，并在此过程中不断丰富甚至修正零信任的内涵和外延，让零信任架构更加成熟，更加实用。

本书的主要译者还有奇安信集团身份安全实验室的张泽洲、蔡冉、沈韵、张丽婷等人，他们既是零信任架构理念的倡导者，也是零信任架构技术方案在国内大型企业落地部署的实践者。在实践过程中，他们对于零信任架构有了更加深刻的理解和认识，特别是针对国内大型部委和企业的 IT 技术架构，零信任架构落地部署需要更多特殊的安全视角和权衡。因此，本书关于零信任架构的某些技术实践细节并不一定完全适用于国内的 IT 技术环境，需要根据实际情况加以修正和补充。幸运的是，零信任架构本就是一个抽象、开放并不断发展的安全框架，对零信任架构的内涵和外延有不同的理解和认知无伤大雅。但是，为了尽可能准确、系统、完整地介绍本书作者对零信任的认知和实践，我们在繁忙的工作之余通读了本书英文原作，在忠于原著的基础上尽最大努力将其翻译成通俗易懂的中文。即便如此，碍于技术理解，以及文字表达能力有限，本书在翻译过程中难免有疏漏和谬误之处，也欢迎读者朋友们批评指正。

此外，在零信任架构理念和技术方案在国内推广实践过程中，奇安信集团的邬怡、韩永刚、张聪、韩笑等人给予了我们非常大的支持和帮助，在此一并致谢！

左英男

2019 年 3 月 15 日

前言

感谢阅读本书！在充斥着威胁的网络中构建可信的系统，是网络安全从业者多少年来孜孜以求的目标。在设计和构建可信系统的过程中，人们在解决一些根本性安全问题时遇到了挫折，而这些安全问题一直困扰和折磨着网络安全从业者。因此，我们非常希望业界同仁直面这些根本性的安全问题，更加积极主动地推进能够解决这些问题的安全系统的建设。

为了实现这个目标，建议在建设和维护安全的计算机网络时采取全新的立场：安全应当与系统的运营管理从根本上融为一体，而不是建立在系统之上；安全应当自始至终与系统并存，要为系统赋能而不能成为其运行的障碍。正因为如此，本书提出了一系列在系统设计时需要考虑的安全设计模式和注意事项，以使得系统具备足够的安全弹性，能够应对现今主流的攻击。

将这一系列设计模式和注意事项作为一个整体，得到的就是零信任模型。在这个模型中，默认的信任是不存在的，每一个访问请求，无论是来自咖啡馆里的一台个人终端电脑，还是来自数据中心的一台服务器，都需要经过严格的检查，并确认其拥有合法的授权。采用零信任模型，可以从根本上解决外部攻击者在网络中的横向移动问题、令人头痛的 VPN 配置管理问题，以及防火墙集中式安全策略管理带来的管理开销问题等。零信任模型与传统安全模型存在根本性的差别，我们深信它代表着网络和基础设施安全架构的未来。

网络安全是一个技术复杂且快速变化的工程领域。网络安全从业者需要深入理解系统多个层面的技术，并明确系统各个层面的漏洞和缺陷，因为攻击者往往正是利用这些漏洞和缺陷来破坏系统的访问控制和保护措施。安全的复杂性与多变性给系统的安全防护带来极大的挑战，但同时也给我们带来极大的成就感，并使我们享受不断学习、应对挑战的乐趣！

本书的目标读者

你是否已经发现，采用集中式安全策略管理的防火墙在实际应用中存在很多限制，甚至遇到过在某些特定情况下无法有效地管理、运营防火墙的情形？你是否在VPN管理上遇到过令人头疼的问题，如多应用和多语言情形下的 TLS 配置问题、合规

审计问题等？这些问题仅仅是零信任模型试图解决的一小部分问题。如果你正在思考有没有更好的办法来解决这些问题，那么你很幸运——这本书适合你。

网络工程师、安全工程师、CTO 等，每个人都可以从零信任模型的学习中受益。即便没有相关的专业背景知识，也可以很容易地理解本书描述的许多原则。本书能够帮助领导者理解零信任模型的基本概念，在零信任模型的实践中做出正确的决策，从而逐步改善组织的整体安全状况。

此外，如果具有配置管理系统（Configuration Management System, CMS）使用经验，会发现可以使用与 CMS 类似的想法构建更加安全、更容易运营的网络，使得网络中的资源在默认情况下得到很好的安全防护。在这种全新的网络设计中，自动化系统如何助力细粒度访问控制的广泛应用，也是一个备受关注的问题。

最后，本书还探讨了零信任网络成熟应用的设计要点，以帮助那些已经采纳零信任理念的组织进一步增强其安全系统的鲁棒性。

本书的写作目的

2014 年，我们开始在行业会议上谈论我们在系统和网络设计中采用的新方法。当时，我们使用 CMS 严格定义系统的状态，以编程方式处理网络拓扑的变更。结果，在使用自动化工具的过程中，我们发现可以用编程的方式处理网络执行的细节，来代替人工管理这类配置。同时还发现，用这种方式自动化获取系统的设计，能够让我们比过去更加轻松地部署和管理安全特性，比如访问控制、加密等。此外，这样做还有更大的好处：在构建安全系统时极大地降低了对网络信任的依赖，这是在公有云或混合云场景下设计安全系统时需要考虑的关键因素。

大约在同一时期，Google 发布了 BeyondCorp 项目的第一篇论文，阐述了 Google 在系统和网络安全设计方面的重新思考，目的是消除对网络信任的依赖性。从这篇论文中发现，Google 试图解决的安全问题、设计安全架构的理念等，在许多方面与我们自己设计的安全系统非常相似。很显然，降低对网络信任的依赖性，不只是我们自己的设计偏好，也是整个安全行业的发展方向。通过比较 BeyondCorp 论文和我们自己的工作，我们的理解也更加深刻，并开始在各种会议上分享这种安全架构和安全理念。与会者都对我们正在做的事情非常感兴趣，但我们也经常听到这样的问题：“我也想在系统中实践这种安全理念和架构，在哪里可以学习和了解详细内容？”遗憾的是，我们的回答通常是“嗯，好像渠道不是很多……这样吧，可以来找我们讨论。”缺乏公开的信息和指导渐渐成为这一安全理念和安全架构推广的障碍，于是，我们决定撰写这本书来改变这种局面。

在本书的撰写过程中，我们访谈了数十家企业的相关人员，了解他们对网络安全设计的看法。我们发现，其中不少企业已经采取了大量的措施，努力减少对其内部网络的信任。不同的公司在设计安全系统时采用的方法不尽相同，但是很明显，他们的工作都是在类似的威胁模型下展开的，因此构建出的解决方案有许多共同之处。

本书的目标不是阐述一两个特定场景的安全设计方案，而是试图定义一个建立在“不可信网络”基础上的安全模型。因此，本书的侧重点不是介绍具体的软件或实现方式，而是探讨零信任网络的理念和基本概念。通过阅读本书，希望你能够理解零信任模型的基本概念，建立清晰的思维模型并利用这一思维模型设计和建设安全系统，甚至构建针对这类问题的可重用的解决方案。

零信任网络现状

零信任模型这个概念最初是由 Forrester 的分析师 John Kindervag 于 2010 年提出的。多年来，他一直致力于建立零信任网络的架构模型和指导原则，并为许多大型企业提供咨询，帮助它们从当前的安全状态逐步演进到零信任网络。John 一直是这个领域的重要参与者，他的工作极大地促进了我们对零信任网络的理解。非常感谢 John 在零信任模型形成初期的大力普及和推广。

目前零信任网络主要是利用现有的软件组件和定制化软件，以全新的方式集成在一起构建起来的。因此，部署零信任网络并不像安装和配置现成的软/硬件那么容易。希望你在学习零信任网络时意识到这一点。

从另一方面来说，缺少易于部署且能够很好地协同工作的组件也是一个机会，一套开源工具可以推动零信任网络的广泛采用。

本书的主要内容

本书的内容组织如下。

- 第 1 章和第 2 章讨论了零信任网络的基本概念。
- 第 3 章和第 4 章探讨了成熟的零信任网络中常用的两个新概念——网络代理和信任引擎。
- 第 5 章~第 8 章详细描述了如何在网络的各个参与方之间建立信任。这些章节探讨的大多数内容都聚焦在现有的技术上，即使是传统的网络安全模型也可以使用。
- 第 9 章将之前讨论的技术集成在一起，探讨如何构建零信任网络，并给出了两

个案例分析。

- 第 10 章则从攻击者的视角审视零信任模型，探讨如何解决网络安全问题。

排版约定

本书采用下列排版约定。

斜体

表示新词、E-mail 地址、文件名，以及文件扩展名。

等宽

用于程序列印，以及在文字中表示命令、模块和程序元素，如变量或函数名、数据库、数据类型、环境变量、语句和关键字。

等宽加粗

表示命令或其他需要用户原封不动输入的文字。

等宽斜体

表示需要被替换成用户指定的值或根据上下文决定的值。

表示提示或建议。

表示一般附注。

表示警告或注意。

Safari® 在线图书

Safari 在线图书（Safari Books Online）是一个面向企业、政府、教育工作者和个人的会员制培训和参考平台。

会员可以访问来自 250 多家出版商的数千本图书、培训视频、学习路径、互动教程以及策划列表，出版商包括 O'Reilly Media、Harvard Business Review、Prentice Hall Professional、Addison-Wesley Professional、Microsoft Press、Sams、Que、Peachpit Press、Adobe、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 和 Course Technology 等。欲获得有关 Safari Books Online 的更多信息，请登录其网站查询。

联系方式

如果你想就本书发表评论或有任何疑问，敬请联系出版社：

O'Reilly Media, Inc.

1005 Gravenstein Highway North

Sebastopol, CA 95472

800-998-9938 (美国或加拿大)

707-829-0515 (国际或本地)

707-829-0104 (传真)

关于本书的勘误、示例和其他信息，请访问官方页面。

关于本书的技术性问题或建议，请发邮件到：bookquestions@oreilly.com。

了解更多有关我们的图书、课程、会议的信息以及最新动态，请访问我们的官方推特，也可以在 Youtube 上观看。

致谢

感谢本书的编辑 Courtney Allen，谢谢她在本书写作过程中给予的指导和帮助。还要感谢 Virginia Wilson、Nan Barber 和 Maureen Spencer 在本书审校过程中的努力和付出。

在撰写本书的过程中，我们有机会和许多人一起讨论其中的内容，感谢他们提出建

议并把该领域其他人的工作情况介绍给我们。感谢 Rory Ward、Junaid Islam、Stephen Woodrow、John Kindervag、Arup Chakrabarti、Julia Evans、Ed Bellis、Andrew Dunham、Bryan Berg、Richo Healey、Cedric Staub、Jesse Endahl、Andrew Miklas、Peter Smith、Dimitri Stiliadis、Jason Chan 和 David Cheney。

特别感谢 Betsy Beyer 为本书编写了 Google BeyondCorp 的案例分析部分！

感谢我们的技术审稿人 Ryan Huber、Kevin Babcock 和 Pat Cable，你们的意见非常有价值。再次感谢你们抽出宝贵的时间仔细阅读本书的初稿。

Doug 在本书的写作过程中花费了大量的时间，因此要感谢他的妻子 Erin、女儿 Persephone 和 Daphne，感谢她们的理解与支持。

Evan 要感谢他的伴侣 Kristen 在本书写作过程中的支持和帮助，还要感谢 Kareem Ali 和 Kenrick Thomas，没有他们的支持与帮助，本书不可能问世。

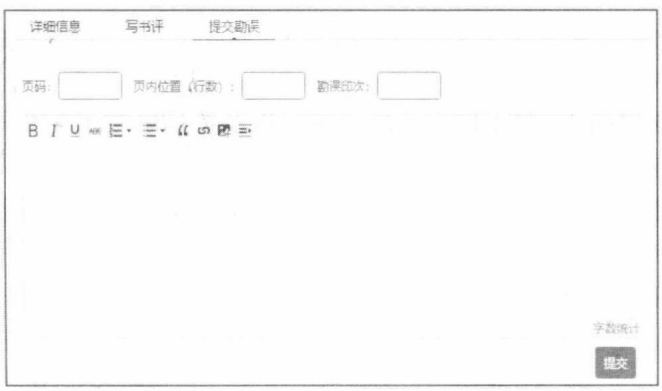
资源与支持

本书由异步社区出品，社区（https://www.epubit.com/）为您提供相关资源和后续服务。

提交勘误

作者和编辑尽最大努力来确保书中内容的准确性，但难免会存在疏漏。欢迎您将发现的问题反馈给我们，帮助我们提升图书的质量。

当您发现错误时，请登录异步社区，按书名搜索，进入本书页面，点击“提交勘误”，输入勘误信息，点击“提交”按钮即可。本书的作者和编辑会对您提交的勘误进行审核，确认并接受后，您将获赠异步社区的 100 积分。积分可用于在异步社区兑换优惠券、样书或奖品。



扫码关注本书

扫描下方二维码，您将会在异步社区微信服务号中看到本书信息及相关的服务提示。

与我们联系

我们的联系邮箱是 contact@epubit.com.cn。

如果您对本书有任何疑问或建议，请您发邮件给我们，并请在邮件标题中注明本书书名，以便我们更高效地做出反馈。

如果您有兴趣出版图书、录制教学视频，或者参与图书翻译、技术审校等工作，可以发邮件给我们；有意出版图书的作者也可以到异步社区在线提交投稿（直接访问 www.epubit.com/selfpublish/submission 即可）。

如果您是学校、培训机构或企业，想批量购买本书或异步社区出版的其他图书，也可以发邮件给我们。

如果您在网上发现有针对异步社区出品图书的各种形式的盗版行为，包括对图书全部或部分内容的非授权传播，请您将怀疑有侵权行为的链接发邮件给我们。您的这一举动是对作者权益的保护，也是我们持续为您提供有价值的内容的动力之源。

关于异步社区和异步图书

“异步社区”是人民邮电出版社旗下 IT 专业图书社区，致力于出版精品 IT 技术图书和相关学习产品，为作译者提供优质出版服务。异步社区创办于 2015 年 8 月，提供大量精品 IT 技术图书和电子书，以及高品质技术文章和视频课程。更多详情请访问异步社区官网 https://www.epubit.com。

“异步图书”是由异步社区编辑团队策划出版的精品 IT 专业图书的品牌，依托于人民邮电出版社近 30 年的计算机图书出版积累和专业编辑团队，相关图书在封面上印有异步图书的 LOGO。异步图书的出版领域包括软件开发、大数据、AI、测试、前端、网络技术等。

异步社区

微信服务号