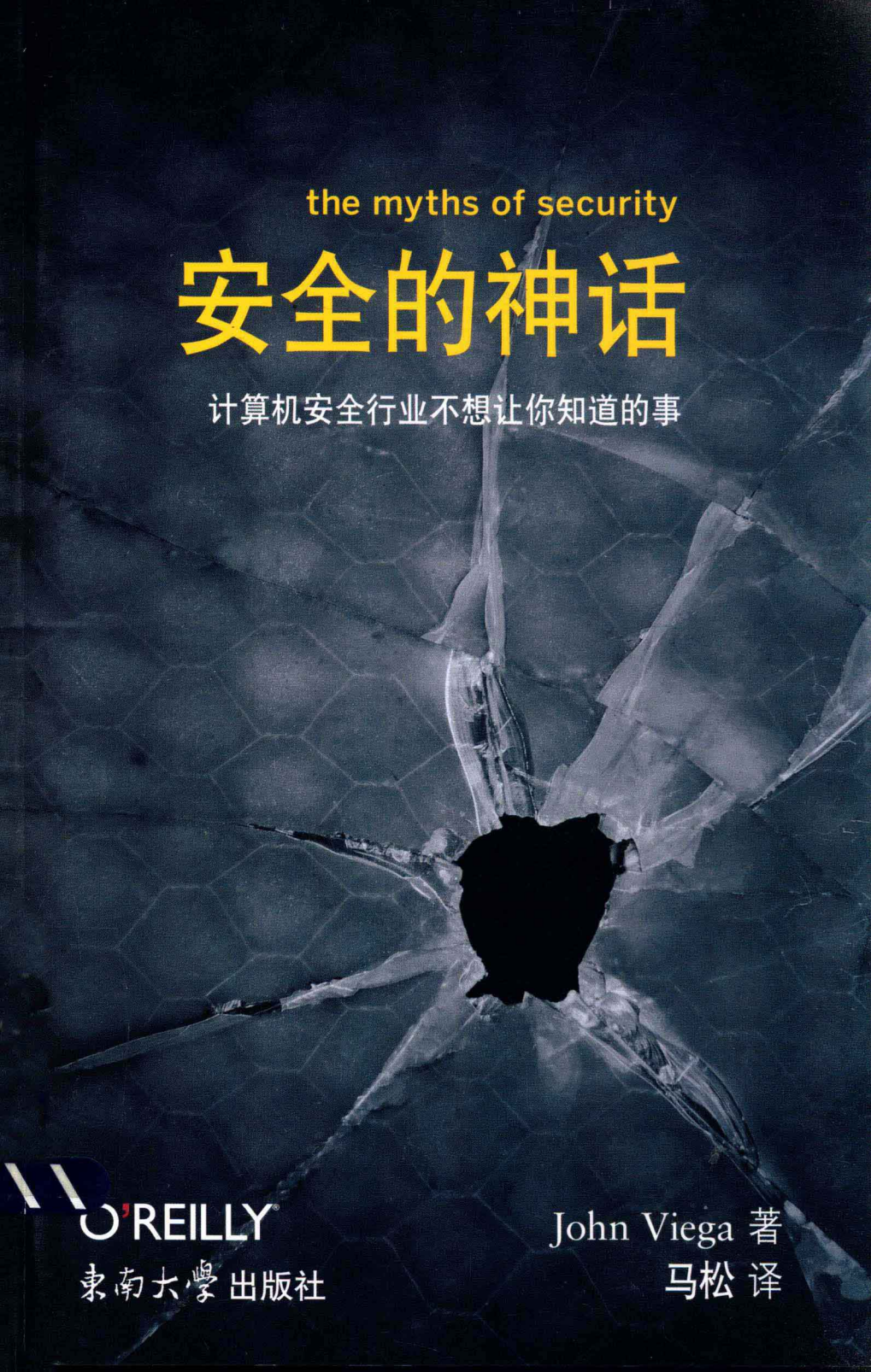
the myths of security
安全的神话
计算机安全行业不想让你知道的事
O'REILLY
東南大學出版社
John Viega 著
马松 译

安全的神话

The Myths of Security

John Viega 著

马 松 译

O'REILLY®

Beijing • Cambridge • Sebastopol • Tokyo

南大学出版社出版

南京·东南大学出版社

图书在版编目（CIP）数据

安全的神话/（美）卫加（Viega, J.)著；马松译.—南京：东南大学出版社，2013.5

书名原文：The Myths of Security

ISBN 978-7-5641-3917-9

I. ①安… II. ①卫… ②马… III. ①互联网络－安全技术 IV. ① TP393.408

中国版本图书馆 CIP 数据核字（2012）第 285444 号

江苏省版权局著作权合同登记

图字：10-2010- 449 号

安全的神话（中文版）

出版发行：东南大学出版社

地　　址：南京四牌楼 2 号　　邮编：210096

出 版 人：江建中

网　　址：http://www.seupress.com

电子邮件：press@seupress.com

印　　刷：扬中市印刷有限公司

开　　本：890 毫米 × 1240 毫米　32 开本

印　　张：9.5 印张

字　　数：247 千字

版　　次：2013 年 5 月第 1 版

印　　次：2013 年 5 月第 1 次印刷

书　　号：ISBN 978-7-5641-3917-9

定　　价：42.00 元（册）

本社图书若有印装质量问题，请直接与营销部联系。电话（传真）：025-83791830

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；创办《Make》杂志，从而成为DIY革命的主要先锋；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。无论是书籍出版、在线服务还是面授课程，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凭借一系列非凡想法（真希望当初我也想到了）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

序

每位计算机用户或多或少都应该担心黑客可能会闯入自己的机器并窃取私人数据。毕竟，计算机软件是复杂并且有许多漏洞的——何况人们还会被伪装得很好的伎俩所欺骗。试图弄清楚计算机安全这一困难的问题让人感到力不从心，所以大家需要一个有效、易用、不会影响用户机器性能的安全产品。

计算机安全行业本应该扮演拯救者的角色。但在本书中，John Viega揭示了为什么会有很多人身处本来可以避免的险境之中。当计算机安全行业把责任归咎于坏蛋，甚至是计算机用户的时候，John Viega正确地指出了安全行业的问题。本书中有很多直言不讳的批评，希望能够让这个行业自省并产生一些积极的变化。如果安全厂商们不再为黑客提供闯入计算机所需的一切工具［在迈克菲（McAfee）[译注1]这是不可接受的］，而且大体上这个行业中的企业之间有更多的

译注1 McAfee，计算机安全公司，设计、生产包括个人计算机杀毒软件在内的安全产品，总部位于美国加利福尼亚州圣塔克拉拉市，2010年被英特尔收购。

合作以尝试解决问题而不是掩盖症状，那将是一个美好的世界。

本书让我觉得骄傲，因为它表明在我担任迈克菲的首席技术官期间，我们所做的工作位居行业的前列。当John抱怨反病毒系统的问题时，他说的都是其他厂商的问题，而且迈克菲已经在用业界领先的技术致力于解决这些问题，比如Artemis[译注2]。当迈克菲用Artemis改变游戏规则时，我可以说这正是在培育更好的技术，甚至将超越John在本书中所描述的反病毒理想境界的远景。目睹这些技术的诞生我感到兴奋，不仅因为它们是在我的关注下培育的，更因为它们用正当的方式从根本上改变了游戏规则。

尽管最近我已经从迈克菲退休了，但基于几个核心的原因我仍然坚信这家公司比业界的其他公司要做得好很多。第一，它是一家专注于安全的公司。从实践的角度讲，迈克菲的智慧不会用在其他的技术上面，比如存储。第二，它关心每一个需要保护的人，从普通消费者到企业客户。迈克菲频繁邀请消费者来参加会议，花很多时间倾听他们的声音。第三，迈克菲雇用了业界最好、最聪明的人才。尽管它有很多的专家， 但迈克菲所做的不是仅仅在收集人才，而是真正地倾听这些人才的声音。当你花很多时间同时倾听专家和你试图保护的人的声音时，你能变得聪明，并能把工作做到令人惊讶的优秀程度。我所热爱的是创造真正的方案来解决真正的问题，而不是头痛医头，脚痛医脚。

能拥有如此多的专家，如John Viega，是迈克菲的运气。John为迈克菲做出了杰出的贡献，领导了很多新兴领域的工作，比如网络防护、防止数据丢失以及软件即服务（Software-as-a-Service）。同时他也在推动核心技术发展和加强实践方面扮演了关键角色。

译注2 *http://www.mcafee.com/us/enterprise/products/artemis_technology/index.html*。该链接原来位于文章中，为方便读者阅读，特将其移动至脚注中。

与John加入迈克菲之前相比，这些工作为迈克菲提供了更好的反病毒和产品安全技术。

我的哲学是一直致力于做到更好，以及总是努力让客户满意。通过与客户的紧密合作，不仅可以了解他们的问题所在，而且可以跟他们建立这样一种关系：不但允许客户对开发活动提出反馈意见，还要鼓励他们提出这些反馈意见。产品并不是诞生于真空。许多其他厂商仅仅依赖他们的聪明伙计，并不多多听取客户的意见，这让他们制造的问题比解决的问题更多。而有些公司，决策的出发点完全基于金钱和公司效益。我和John都不认同这些做法，John坚持为公司以及客户做正确的事情。

对于John和我自己而言，客户是第一位的。我们总是尽自己最大所能去做得更好。比如，我们已经推动迈克菲发布免费的软件，例如SiteAdvisor和Stinger恶意软件清除工具。总有些厂商通过把软件缺陷公之于众来获得利润，却把用户置于危险的境地，而John和我则总是致力为每一位软件用户做正确的事情。当我在迈克菲任职的时候，如果员工在别人的代码里面发现一个缺陷，我们的措施是去通知相关厂商，而不是通知全世界。（我们也会建议厂商不要公布这一问题，尽管他们常常并不听从这个建议。）而如果某些事情的确公布了，我们会提供免费的信息来帮助人们判断是否身处危险之中。

John的哲学是为客户做对的事情，这是绝对正确的。我希望整个安全行业都认同这个想法。或许这本书可以使行业中其他公司警醒。

通过为客户提供宝贵的帮助，John的领导力已经让他在迈克菲产品的各个方面都留下了烙印。他不惧怕做对的事情，即使这件事情不受欢迎。而且他也不惧怕为整个计算机安全领域发出“行动呼吁”，这正是他在《安全的神话》一书里所做的事情。我谨希

望业界同仁也用跟我同样的角度来看待这本书，并将它当做建设性的批评以为每个人都建立更好的安全。基于我在这个领域过去15年多的丰富经验，能被我放到这个位置的书是寥寥无几的。当我与其他人谈论计算机安全领域时，我肯定会向他们建议阅读本书。

——克里斯托弗·波林（Christopher Bolin）
迈克菲前首席技术官和执行副总裁

前言

《安全的神话》是为任何对计算机安全感兴趣的人所写的书，无论这个兴趣是出于爱好、职业需要或者只是某些令你担心的事物。通过阅读本书，你将深刻了解坏蛋们做什么事以及好小伙（还有好姑娘）做什么事。你会发现好人经常办坏事——这些坏事把大家都置于危险之中。你还会了解到计算机安全行业一直以来都搞错了什么事情，并且它如何慢慢开始发生变化。

如果你已经拿起了本书，很大概率表明你对计算机安全的关心已经大大超过平均水平。每当安全行业以外的人问起我的职业时，我的回答总是激起以下三种反应的其中之一：

- 他们漠不关心地看我一眼并解释为什么他们不关心这个问题。比如，“我用苹果计算机（Mac）”或是“我让年轻人替我操心这个”。
- 他们问诸如 “我该做什么来保障自己的安全？”这类的问

题，而当我给出答案时，他们就转换话题了，因为他们以为自己已经知道关于互联网安全的所有答案了。

- 他们给我讲发生在他们的计算机上的“恐怖事件”并问我能不能帮上点什么。

很多人很聪明，也精通计算机技术，但就是不关心安全问题，除非某些问题的发生可能影响到他们。他们愿意少量付出以让自己的计算机运行良好，但这些付出应当不会引起更多麻烦。例如，如果反病毒软件消耗过多资源而让计算机变得太慢时，一些人就会把反病毒软件停掉。

当你进入IT（信息技术）行业，你会发现很多人似乎对安全很感兴趣。它就像一个令人难以置信的挑战游戏。坏蛋是狡诈的，总是找到很多方法（常常是令人难以置信的创造性方法）来绕开其他人设置的所有防御。我们需要建造更好的防御系统以让坏蛋们少一些成功。

这是一个我们无法一直赢的游戏。

试想假如你要保护整个因特网，其中至少有16亿用户。我们假设每位用户的安全机制都是99.9%有效，并且至少每年遭到一次攻击。即便如此，一年仍然有160万的用户被感染。

从好的方面说，人们并不是时常遭到攻击。从坏的方面讲，安全防御失败一次就够让你身陷麻烦之中。只要涉及金钱，就总有人不惜为之铤而走险。并且，就算一个IT系统没有什么周知的安全隐患，坏蛋也会为达目的不惜撒谎、欺骗并偷窃。记住，坏蛋们在接触计算机前就得手了，而且会想尽办法找出最简单的途径。

如果你真正想知道的就是怎样才能保护自己，我在后续章节中的确涵盖了这方面的内容。但如果你不想看那么多，那以下的三个

步骤大概可以保你平安：

1. 运行当前机器上的反病毒软件（当你的反病毒软件更新订购过期时不要忽略不管）。
2. 总是为你所使用的操作系统和应用程序安装更新，越快越好。
3. 在因特网上做任何事情之前，确认你是在跟合法的人员打交道，无论是在线购物、打开你所接收邮件的附件或者运行一个从网上下载的程序。

现如今，除非反病毒软件报警，否则你不会注意到计算机被病毒感染了，此时反病毒软件多半能够清除感染。但如果你的计算机似乎变得一团糟时（如莫名其妙地系统崩溃、运行缓慢、弹出很多广告），或许就是感染病毒了。这些情况下，正确的选择是找一个你信得过而且有能力处理这些问题的人帮你。这个人可能是你的孩子，或者是百思买（Best Buy）的“极客小队（Geek Squad）”。在最坏情况下，你的计算机可能就需要重新安装系统了，所以经常备份计算机里的数据也是一个不错的点子（尽管此时备份的建议听起来有点老生常谈）。

如果你首要考虑的是保障自己的安全，那到此为止你已经学到所有你需要知道的东西了，而这些可能都不是什么革命性的东西。无论如何，希望你有足够的好奇心再往下看一些，并了解更多有关计算机安全行业的知识。IT行业中的那么多人认为安全问题有趣是有原因的，而如果你读下去，或许你就明白了。

安全行业有足够大的市场空间，每年吸引超过100亿美元的资金。其中有数百家公司和上千种产品。大多数计算机用户需要关注安全问题。IT安全市场很大的一个部分是集中在将解决方案销售给企业。一旦企业变得更大，就倾向于雇用具有一定安全知识的人来负责选购公司使用的安全技术。在本书中，对于这种类型的读

者，我并不打算过多考虑他们的需求，哪怕这些人有足够好的理由来考虑IT安全（保住职位）。尽管在公司领域有太多的神话需要揭穿，但我的兴趣更多地倾向于解答普通用户的问题。

此外，大部分普通用户不需要操心诸如遵守萨班斯－奥克斯（Sarbanes-Oxley）法案或者来自不同安全厂商组成的管理委员会能否在彼此之间共享数据这样的事情。

为何要写《安全的神话》？

在计算机安全这样一个混乱和模糊不清的学科里孕育神话是很自然的一件事情。在本书中，我将厘清很多那一类的神话。

大多数人听过——并且可能相信——某些神话就是计算机安全行业自己炮制出来的。比如，曾经有很多非技术人员问我："迈克菲真的是自己先制造病毒然后再报告给用户吗？"（不是。）很多人可能都听说Mac要比Windows PC更安全，但事实要复杂得多。并且，大家都设想自己计算机上的反病毒软件正在保护着系统，但这一点是值得怀疑的。

安全行业的从业人员也有自己的错误观念。每个人似乎都认为漏洞研究社区正帮助提高安全性。但这不是真的，漏洞研究为坏蛋提供了便利。

对于这些问题我将讨论我的一些解决方案。我们认为很多这样的问题是难以处理的。正如我所说，坏蛋有天生的优势——但这并不意味着没有对付他们的办法。

致谢

为了鼓励我妈妈来读此书（她很聪明，但也许自认为可以不考虑安全问题， 因为她用Mac），我将此书献给她。我非常幸运，在我的人生中认识很多了不起的人，这些人鼓励并信任我，而我妈妈是其中认识最久的。而且我知道她也是做得最棒的，因为没有什么比父母对孩子的爱更强烈。

我应该知道，因为无论我的女儿们，艾米莉（Emily）和莫莉（Molly），多么坚持地认为她们爱我胜过我爱她们，我都知道那是绝不可能的。谢谢孩子们，因为你们出色的表现。你们让我比你们想象得更快乐……这种快乐等到你们某天有了自己的孩子就会明白。并且，如果你们有孩子的话，我希望你们的孩子就像你们现在这样。通常当父母们这么说时，是因为孩子让他们觉得辛苦，所以他们要让孩子知道做父母是如何地不易。这里完全不是这样的意思。你们这些小朋友从没有让我觉得辛苦，做你们的父亲总是很轻松。我仅有的一点点遗憾，那是因为与现状相比，我希望我们能花更多的时间在一起。

一天之内绝无可能有足够的时间来完成一切。写一本书也不例外。一个人用来写作的时间一定来自于某处。对我而言，那就意味着我花在工作上的时间少了。所以我要感谢布雷克·瓦茨（Blake Watts）帮我弥补了我在工作上的懈怠之处，感谢他很早就审阅了本书的很多部分，还要感谢他的积极乐观，哦，当然也感谢他的出色贡献。

同样，我也要感谢我令人着迷的女友，黛比·莫伊丽罕（Debbie Moynihan）， 无论何事她都对我宽容以待。显然我并不是最棒的男朋友，因为我花了太多的工夫在工作和这本书的写作上，但她从未抱怨过，相反，她帮我审阅了整部手稿。我真是个幸运的人。