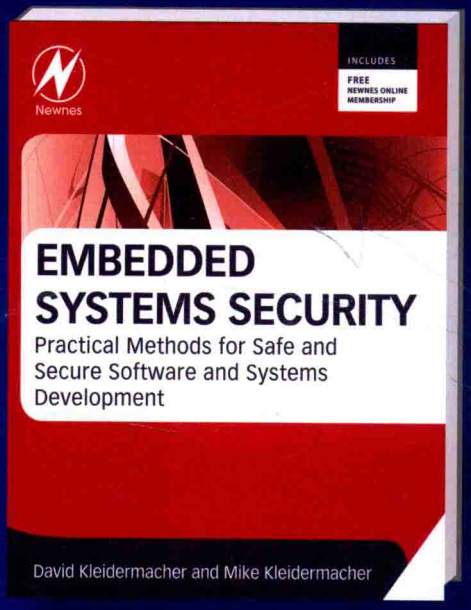
HZ BOOKS
华章科技

ELSEVIER
爱思唯尔

首本嵌入式系统安全领域的书籍，填补了国内此领域的研究空白。
从软件架构、加密、数据保护以及应用等方向进行全面而深入的剖析。
本书作者系NSA加密认证系统首席设计师，拥有丰富的嵌入式安全经验。

电子与嵌入式系统
设计译丛



Embedded Systems Security
Practical Methods for Safe and Secure Software
and Systems Development

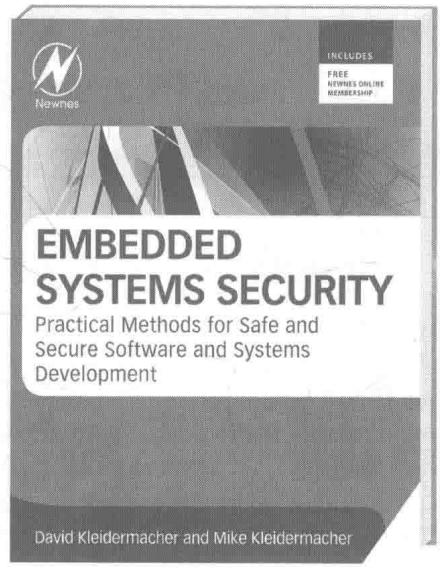
嵌入式系统安全

安全与可信软件开发实战方法

［美］戴维·克勒德马赫（David Kleidermacher）
迈克·克勒德马赫（Mike Kleidermacher）著
周庆国 姚琪 刘洋 严凤龙 等译

机械工业出版社
China Machine Press

电子与嵌入式系统
设计译丛



Embedded Systems Security
Practical Methods for Safe and Secure Software
and Systems Development

嵌入式系统安全

安全与可信软件开发实战方法

[美] 戴维·克勒德马赫（David Kleidermacher）
迈克·克勒德马赫（Mike Kleidermacher） 著

周庆国 姚琪 刘洋 严凤龙 等译

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

嵌入式系统安全：安全与可信软件开发实战方法 /（美）克勒德马赫（Kleidermacher, D.），（美）克勒德马赫（Kleidermacher, M.）著；周庆国等译 . —北京：机械工业出版社，2015.11
（电子与嵌入式系统设计译丛）
书名原文：Embedded Systems Security: Practical Methods for Safe and Secure Software and Systems Development

ISBN 978-7-111-52007-8

I. 嵌… II. ① 克… ② 克… ③ 周… III. 微型计算机－系统开发－安全技术 IV. TP360.21

中国版本图书馆 CIP 数据核字（2015）第 253963 号

本书版权登记号：图字：01-2014-4753

嵌入式系统安全：安全与可信软件开发实战方法

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号　邮政编码：100037）

责任编辑：佘　洁　谢晓芳　　责任校对：殷　虹

印　　刷：三河市宏图印务有限公司　　版　　次：2015 年 11 月第 1 版第 1 次印刷

开　　本：186mm × 240mm　1/16　　印　　张：18.25

书　　号：ISBN 978-7-111-52007-8　　定　　价：79.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

客服热线：（010）88379426　88361066　　投稿热线：（010）88379604

购书热线：（010）68326294　88379649　68995259　　读者信箱：hzit@hzbook.com

推 荐 序

《嵌入式系统安全》这本书是我在两年前看到并推荐给机械工业出版社张国强先生的，很高兴这本书翻译完成并很快要印刷出版了。

从本书的英文书名《Embedded Systems Security: Practical Methods for Safe and Secure Software and Systems Development》不难看出本书的两个特点。第一，实践性强。作者 David Kleidermacher 是嵌入式安全领域中著名的专家，在书中他与读者分享了他的知识和长期的经验。Kleidermacher 于 1991 年加入 Green Hills Software，这是美国加州的一家著名嵌入式软件公司，以开发高可靠性与安全性的操作系统与软件工具而闻名世界，他曾经是公司系统软件工程师和 CTO。2015 年 2 月，Kleidermacher 被 BlackBerry（黑莓）公司任命为 CSO（首席安全官），负责公司安全相关的产品研发和组织。本书的实践性还体现在第 6 章，该章讲述了包括汽车电子和 Android 的安全性等热门主题。第二，范围广泛。书中反复提到的 Safe 和 Security，翻译成中文可能都是安全一词，但二者的含义还是有区别的。前者更多意味着系统的可靠性（在第 2 章和第 3 章中），国外称为功能安全，后者是我们目前谈论更多的信息安全性（在第 4 章和第 5 章中）。其实二者之间不是孤立的，亦有紧密的联系，比如第 2 章中的系统管理程序（Hypervisor）和虚拟化技术既可以应用于嵌入式系统可靠性设计，也可以应用于嵌入式网络安全产品设计，这些内容在本书中都有详细讲述。

为什么要推荐本书？两年前我正在翻译《嵌入式软件精解》（英文书名是《Embedded Software, Second Edition: The Works》）一书，《嵌入式软件精解》与《嵌入式系统安全》同为 Elseviser 出版社的 Newnes 系列丛书，我对这个系列的图书印象很好，它们很专业和实用。今天嵌入式安全方面的图书依然非常少，本书是我看到的在系统和软件方面写得非常好的一本。

最近几年物联网（Internet of Things，IOT）风起云涌，联网后的嵌入式系统安全性问题更加严峻和急迫，面向物联网安全设计，本书翻译并出版的意义就更大了，也非常及时。物联网的安全性考虑归纳起来有下面几个方面。

第一，容易被攻击的对象更多了。比如家电联网变成智能家居了，汽车联网变成车联

网，那么汽车和家电可以成为被攻击对象，这里汽车是指广义的运输工具，包括公共交通，甚至飞机（我最近乘坐过美联航（Bluejet 航空），它们都已经提供机内 Wi-Fi 服务）。

第二，更多日常活动因为攻击而可能中断。除了汽车和家电之外，大量可穿戴的医疗健康设备，都通过智能手机接入互联网，攻击导致设备故障或将危机人们的健康甚至生命。

第三，互联网和大数据通过传感器收集到了关于物的大量信息，其内容更加广泛，如果信息泄露危害更多。比如我们驾驶的汽车的位置和我们的使用习惯，个人体征和疾病信息，以及智慧城市的建筑和交通等管理信息，它们都可能被泄露。

第四，若电网、交通运输和交通管理、核电站和环境监测等关键系统遇到黑客的攻击，就会具有毁灭性的危害。

第五，新的开放标准与传统的私有标准之间的转换带来的安全隐患。比如物联网设备中使用的 ZigBee、Z-Wave、Thread 和 ANT 协议与互联网的 IP 协议之间的转换，国际性标准组织 IETF、ITU 和民间企业联盟，比如 OIC 和 AllJoyn（Allseen Alliance），正在架构层做工作期望降低安全风险，但是因为大量的设备已经存在，尚需时间方能完善。

物联网安全性已经引起了学术和工业领域的关注，哥伦比亚大学计算机专业今年春天讲授的网络安全课程已经加入了 IoT 安全性方面的内容。我 2015 年 6 月在旧金山参加的一个嵌入式会议上遇到了一家网络软件公司，它们已经在提供面向工业物联网的嵌入式网络安全软件和架构技术。著名开源技术咨询公司 Blackduck，在其白皮书《物联网与开源软件》中也详细讨论了物联网端点和边缘节点设备的安全问题。

希望本书能让在嵌入式系统和物联网第一线工作的工程师、老师和学生们学习到新的知识与技术；让 IT 和互联网领域的信息安全专家们了解到嵌入式物联网设备安全设计的特殊之处。感谢机械工业出版社再次为国内读者带来一本嵌入式系统专业力作。

何小庆

2015 年 6 月

于美国硅谷和北京海淀中关村

译 者 序

随着现代信息技术的不断进步，嵌入式系统的广泛应用及网络化发展已深入到各个行业。于是，系统的可靠性及其敏感数据的安全性也成为时下人们迫切关注的问题。我国政府充分认识到其重要作用，并在政策、资金等方面给予大力支持。早在2004年，国家颁布的《当前优先发展的高技术产业化重点领域指南》，就已经把嵌入式产业作为国家发展的一个重要领域。

近年来，我国嵌入式系统市场处于快速增长时期，由于嵌入式系统资源的有限性，其安全问题比一般的桌面系统更加复杂。对于安全嵌入式系统，要在整个设计过程中充分考虑安全因素，从而决定采用哪种安全技术。因此，构建一个安全的嵌入式系统的问题研究势在必行。

本书全面、系统地探讨了嵌入式系统安全方面的知识，有助于嵌入式安全领域的从业人员对平台组件安全有深入的了解。重点对关键系统的软件和硬件问题进行分析，帮助开发人员从整体上建立一个系统安全架构，从而提高产品的安全性和可靠性。本书有以下几个特点：

1）从读者的角度出发，以通俗易懂的语言，结合丰富多彩的实例，详细介绍了嵌入式系统安全开发设计各方面的知识。通过行业标准和实际经验提出切实可行的嵌入式安全方法，这无论对于初学者还是资深开发者来说都具有一定的借鉴和指导意义。

2）从系统层面对嵌入式系统安全进行分析说明，特别是对安全嵌入式软件开发和嵌入式加密等方向进行了细致分析，从安全的整体性出发，为构建嵌入式系统的安全提供依据，从而为开发者提供嵌入式系统安全方案的思路。并且进一步探讨了嵌入式系统数据保护协议及新兴技术，讨论开发安全软件行之有效的技术，实现缩短开发时间和降低成本的目的。

3）选取了大量开发实例及热点事件，如VxWorks调试端口漏洞、Duqu病毒、Stuxnet病毒、沃克间谍案、网络交易、汽车安全和安卓系统安全等。以具体案例深入浅出地分析嵌入式系统安全的问题。

在此译者要非常感谢撰写本书的两位嵌入式系统安全专家，作者David Kleidermacher是

格林希尔软件公司首席技术官，主要负责引导技术战略、平台规划及方案设计。自1991年起，他一直在格林希尔软件公司从事系统软件和安全领域的研究，参与并指导了多种高安全等级的产品。另一位作者Mike Kleidermacher是一位资深电子工程师，45年来他一直致力于安全嵌入式设备的设计、实现及战略演进。并且Mike曾担任过不同的职务，包括项目经理、技术总监、总工程师等，这也使得他能从系统上给读者以指导。

多年来两位专家积累了丰富的开发实践经验，而本书融合了这些宝贵的经验。因此，对于嵌入式安全设备开发人员来说，本书是一本不可多得的实战参考手册。

译者认为本书属于中等级别的嵌入式安全方法——相对全面和细致，但并没有过于深入地对每一个知识点进行介绍。书中所涉及的标准及方法有一定的侧重点，避免了泛泛的讨论，重点集中于可能影响系统安全方面的问题，更偏向于实际问题的解决。对于一些深入的问题，这本书给读者指明了方向并且给出了参考资料。如果读者有兴趣，可以根据资料做深入的研究。

翻译本书是一个团队合作的过程，感谢机械工业出版社张国强的信任和支持。本书由周庆国教授、姚琪、杨柳组织翻译，刘洋、严凤龙、孙晓娟、李飞、石强胜也参与了本书的翻译、审校工作。本书的出版是集体智慧的结晶，感谢各位同仁的不懈努力。

由于时间原因及译者水平有限，本书中不足之处在所难免，恳请读者批评指正。

周庆国

2015年5月于兰州

序

终于完成了！一本关于构建安全嵌入式系统的书终于完成了。

从报纸上，几乎每天你都能看到一连串关于泄露和漏洞利用的故事。信用卡信息从数据库中蹦了出来，个人信息从公司服务器中涌了出来。

但如房间中的大象，真正的威胁载体在很大程度上被忽略了。对于世界上的每一台计算机，都有成百上千的嵌入式系统，这些嵌入式系统通过一系列日益增长的通信信道互联。WiFi、蓝牙、以太网、RFID、FireWire——此类技术数不胜数。智能手机至少有 4 根天线以及可重新擦写的内存，而且如果遭到入侵，可能成为一种电子的“病毒传播者”。

任何有网络连接的设备都可能成为某种威胁的载体。一个 USB 牙刷（是的，至少在市场上有一款这样的产品）可能携带生物的和计算机的感染元素。也可以是一个智能鼠标垫（与计算机互连，可以显示自定义图片）。用来展示你所爱的人的可爱照片的无线电子相框，可能拥有一颗邪恶的“心”，因为它正在“毒害”你的邻居的网络。

考虑到目前一些汽车已经配置了线控制动系统。牵引机配置线控转向已经有一段时间了；方向盘只是一个旋转编码器，这样的技术肯定会引入到汽车中。但是消费者希望在工作、娱乐和路上开车时都能连网。对于一个游遍大半个世界的坏家伙来说，只是通过发送 TCP/IP 数据包就在加州第五号公路（I-5）引起一场灾难性的危机，这样会有多难呢？

显然，这一点也不难。研究人员已经能够通过各种载体控制汽车。

美国国土安全部的工程师远程入侵了一台大型的柴油发电机并摧毁了它。Stuxnet 病毒表明，一个陈旧的监控和数据采集（SCADA）控制系统可能是一个由政府暗中支持的武器。SCADA 系统控制着发电厂、工厂，当然也会涉及任何工业生产。昆士兰的一个污水处理厂遭到攻击，导致有毒液体大面积泄漏。

当电网变得智能时，又会发生什么呢？

至少有一个公司销售的轴承采用了磁场悬挂支撑轴；DSP 芯片差不多每秒执行 15 000 次计算才能让机械平稳运行。而且轴承控制器是通过以太网连接的！协同攻击轴承——就是轴承！——可能使制造业遭受损失。

市场上已经出现联网的烤面包机，也有联网的咖啡机。当1亿美国人在某个星期一的早上醒来，正睡眼朦胧，甚至可能因宿醉而难受，喝过一杯咖啡后完全不起作用，要做的事情将陷入停滞状态。但事实上，他们仍会继续惬意地睡觉，因为某个尼日利亚少年重设了所有的闹钟。

还有另一个安全问题：非恶意的bug。随着嵌入式系统越来越成为文明社会中重要的一部分，任何能够破坏系统可靠性的bug都会成为一个至关重要的安全问题。当监狱自动控制门无法关闭时，监狱就成了酒店，但可不像加州旅馆，因为所有的客人都急着要退房。一项任务如果消耗了太多的资源（如内存）或CPU，它就会阻碍其他活动的运行。交通灯无法变成红灯，而铁路信号一直开着，或ATM的点钞机一直吐钱，无法停下来（有人会这样希望的）。

大多数的嵌入式系统开发人员基本没有接受过安全培训，而且多数不会意识到威胁的存在，从来不知道应该有意识地使用各种技术和技巧使他们的产品更加牢固耐用。本书首次涉及了这样的议题。Dave和Mike Kleidemacher清楚地描述了这些安全问题，并且提出了五项“高可信软件工程原则”指南。需要一份清楚而完整的加密技术介绍，或数据保护的各种细节吗？本书通过丰富的示例对此加以阐述。

很多开发人员放弃了构建一个安全的系统，因为他们认为敌人总是先行一步。而且嵌入式系统不会像计算机一样，能够每隔15分钟升级一次，所以改进的防范措施总是落后于新型的攻击。但Dave和Mike指出，确实有可能构建安全的嵌入式软件。

本书作者认为构建安全的嵌入式系统并不容易。在某些情况下，甚至工具本身都必须经过评估和认可。但是，安全固件将成为国家的当务之急，甚至是国家的一项竞争优势。这本书会给出这些问题的答案。我也希望，该书能够敲响关于安全的警钟。

Jack Ganssle

前　言

关于本书

本书的目的是希望帮助嵌入式开发人员，提高产品的安全性和可靠性。虽然有些图书涉及了嵌入式系统安全，但内容的主题相当狭窄，几乎完全专注于硬件相关问题，或网络安全协议及其底层加密。相比之下，本书旨在实现一种全面的、系统层面的安全：硬件、平台软件（例如操作系统和系统管理程序）、软件开发流程、数据保护协议（网络和存储）以及加密。虽然没有哪个标题能够实际涵盖嵌入式系统安全的每一个话题，但本书尝试解决构建当代嵌入式系统中主要与安全相关的组块。

读者会获得一种对关键系统软件和硬件问题的深刻理解，这些问题是设计安全嵌入式系统必须要考虑的。大多数嵌入式系统开发人员并不会去写他们自己的操作系统和网络协议，也不用设计他们自己的微处理器。因此，精通与这些平台组件安全相关的知识，对做出正确的嵌入式设计选择，特别是在某个特定操作环境下满足安全目标至关重要。

读者将学习一种有效地开发安全嵌入式软件的方法。除了合理地应用平台组件之外，嵌入式开发人员必须设计自己的软件，并且保证以最高可用安全级别的方式集成整个系统。因此，本书的一个重要目标是讨论用于开发安全软件行之有效的实用技术。我们也尝试拆穿这样的“神话”，即为了大大提升软件安全，不可能不投入与之相当的开发时间和成本。书中提出的方法源自行业标准和实际经验的结合。我们相信，嵌入式系统开发人员在这方面严重缺乏高质量的指导。我们的目标是填补这个空白。

读者对象

本书主要面向参与嵌入式系统开发的工程专业人员。硬件、软件和系统工程师，以及架构师多多少少都会涉及嵌入式系统安全。

计算机安全最重要的原则之一是，若系统的最初设计未考虑计算机安全，则改造系统的

安全能力是困难且不明智的，而且常常在经济上或技术上都是不可行的。因此，为了提高嵌入式系统领域的安全性，唯一的希望是指导开发人员，必须学会像思考功能、内存占用和调试一样思考安全问题。

本书还为专业人士提供了一个重要的参考，即关于嵌入式系统的测试和质量保证。这些工程师必须学会测试安全强度，但这方面的挑战要比测试某个功能规范要困难得多。因为即使可能的话，完全列举潜在的安全威胁通常也是很困难的。安全测试需要巨大的创造力和决心。但是，质量控制工程师拥有很多工具可以解决这个问题，而且本书的一个重点是提供此工具箱相关的实用指导。

对于构建安全嵌入式系统的关注必须渗入到组织中。开发人员的培训必须包括阅读像本书一样的教材，参加有安全指导的技术会议，从项目的关键硬件和软件供应商得到的训练，以及经常性地接触相关的时事。因此，本书面向负责确保开发人员设计的安全性的管理团队。管理必须要了解嵌入式安全问题，而且必须成为这种培训的卖点。在汽车的示例中，本书提及的管理要负责单个组件，例如一个信息娱乐系统和这些组件的集成（例如，主要的一级供应商和汽车制造商），以及产品整体的集成。事实上，汽车、飞机、火车、工业控制系统，或任何其他类型的电子产品，都有着大量的嵌入式系统，负责制造这些产品的企业的副总裁、总经理和管理者将因阅读本书受益，并会放在书架上以供参考。

除了与安全相关的专业人士之外，本书也为对可靠性要求较高的嵌入式系统开发人员提供指导，这些系统包括生死攸关的医疗设备、航空电子设备和其他运输系统、通信系统，甚至像智能手机这样大容量、复杂的消费类设备。对于构建安全、可靠的嵌入式系统存在巨大的共性需求。

最后，本书中的很多安全概念，特别是软件开发实践，是与工程专业相关的，但是已经超出了嵌入式系统领域。例如，本书教导 Web 应用程序开发人员，不仅要关心脚本和数据库的漏洞，还要全面了解 Web 服务器可能对操作系统、其他应用程序以及底层的计算机硬件的安全的影响（反之亦然）。

相对资深的工程师和架构师阅读本书也有帮助。但对于入门级的程序员，以及大多数经验丰富却相对缺乏安全问题相关经验的开发人员，这本书对他们是相当有用的。甚至有大量安全背景和知识的工程师可能会发现，本书也有助于完善他们的“知识库”。

虽然本书并没有写成教科书的风格，但对于计算机科学或工程学科中教授或学习嵌入式系统的在校教师和学生也会有帮助。在全球技术学院中，嵌入式系统开发是一门极缺乏的学科，而且几乎没有嵌入式安全的指导。

本书内容安排

我们建议所有读者从头至尾按顺序阅读所有章节。对于那些时间紧迫的人，我们进行了以下梳理，根据工作职能对内容进行了主次之分。

第 1 章讨论了在嵌入式系统中提升安全性的发展趋势，接着介绍了威胁的基本定义以及对抗这些威胁所采取的保护策略。在本质上，我们采用了不同的安全和嵌入式系统观念，并且总结了它们在现代嵌入式系统中的交集。第 1 章还提供了在一些最激动人心、发展迅速而且重要的新型嵌入式系统技术领域中安全概念和指导的示例应用，包括智能手机、智能电网，并展望了嵌入式安全趋势。这一章强烈推荐给所有读者。

第 2 章全面地讨论了安全问题以及与平台软件相关的最佳推荐的应用，包括操作系统、超级管理程序和多重独立安全等级（MILS）架构。该章还讨论了与整个系统安全架构相关的关键安全问题和最佳推荐实践，以及对可用的硬件功能的影响，如 MMU、IOMMU 和虚拟化加速。该章对于工程师、架构师和技术经理最为重要。

第 3 章旨在最大限度地保证嵌入式软件的安全。关键性的原则和指导贯穿了整个章节，因此该章对于软件开发人员以及技术经理最为关键。

第 4 章概述了大多数重要的加密算法、密钥管理和美国政府面向嵌入式系统的相关指导。除了涵盖这些基本内容之外，我们还讨论了嵌入式系统环境下的加密概念以及特有的制约和要求。如果读者没有扎实的密码学基础，都应该阅读该章。即使当前项目没有用到加密功能，但是在将来的项目中也很有可能用到。加密和验证构成了所有数据保密与网络访问保护的基石。

第 5 章涵盖了最重要、最广泛的网络安全协议，例如 IPSec 和传输层安全（TLS）以及存储加密方法，并且强调了在资源有限的嵌入式系统中的实现问题。该章为专业人士在最新安全协议标准及其修订版本方面提供一种介绍或补充。该章核心目的之一是帮助开发人员为涉及安全的相关系统层（网络和存储）制定正确的决策。该章还包括了一些高级议题，例如网络时间信道，有兴趣的读者以此可以了解确保重要资源的机密性。

第 6 章提供了扩展案例的分析，这些都建立在前面章节内容的基础上并加以了应用。该章涵盖了少数新型应用和环境中的安全问题及示例性解决方案架构。第 6 章推荐给所有读者。

致谢

感谢 Guy Broadfoot，感谢他为第 3 章的模型驱动开发部分所做的贡献。

感谢 Jack Ganssle，感谢他为本书写的序言以及他给出的审阅和反馈意见。

感谢 Michael Barr，感谢他的审阅和反馈，以及 Netrino 对《Embedded C Coding Standard》所做的贡献，第 3 章把该书当作一个案例分析进行了讨论。

感谢 Thomas Cantrell、Jack Greenbaum、Dan Hettena 和 Philippa Hopcroft，感谢他们深思熟虑的审阅和反馈。

感谢 Elsevier 公司的编辑 Tim Pitts 和 Charlotte Kent，感谢他们对整个项目的支持。

感谢本书的插图设计者 Tamara Kleidermacher，他煞费苦心地为这本书制作了各种插图。添加可视化手段以辅助技术讨论的能力相当关键，而且 Tamara 对于视觉风格和统一很有天分，大大改善了本书。

Mike 要感谢他的儿子 Dave，感谢他的邀请使其成为这项工作的合作者。

Mike 要感谢 Ellwood (Chip) McGrogan，正是他“教会了我所知道的密码学知识”。

David 要感谢他的家人——Tamara、Hannah 和 Aaron——在编写本书的很多夜晚和周末，感谢他们一如既往的支持和非凡的耐心。

David 要感谢他的哥哥 Paul，作为自己一生的榜样，感谢他坚定不移的鼓励、支持和真诚的忠告。

David 要感谢 Dan O'Dowd 和 Mike Kleidermacher，感谢他们几十年来慷慨地分享和传递他们的知识与激情。

David 要感谢美国格林希尔软件（Green Hill Software）公司曾经的和现在的员工，感谢他们多年来的支持。这个才华横溢的团队让整个世界变得更加美好，更加安全，与他们共事是我的荣耀。

目　录