HZ BOOKS
华章IT

WILEY

信息安全
技术丛书

世界顶级安全专家亲笔撰写，从软件架构视角，全面总结软件开发领域的各类安全模式，覆盖现代安全问题，包含大量真实案例

从概念到设计，再到实现和逆向工程，详细讲解安全模式在开发安全软件过程中的应用，提供详细的实现建议和UML图

安全模式最佳实践

[美] 爱德华多 B. 费尔南德斯 (Eduardo B. Fernandez) 著
董国伟 张普含 宋晓龙 刘晓舟 等译

SECURITY PATTERNS
IN PRACTICE
Designing Secure Architectures
Using Software Patterns

机械工业出版社
China Machine Press

安全模式最佳实践

[美] 爱德华多 B. 费尔南德斯 (Eduardo B. Fernandez) 著
董国伟 张普含 宋晓龙 刘晓舟 邵帅 王欣 辛伟 译

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

安全模式最佳实践 /（美）费尔南德斯（Fernandez, E. B.）著；董国伟等译 . —北京：机械工业出版社，2015.4
（信息安全技术丛书）
书名原文：Security Patterns in Practice: Designing Secure Architectures Using Software Patterns

ISBN 978-7-111-50107-7

I. 安… II. ① 费… ② 董… III. 软件开发 – 安全技术 IV. TP311.52

中国版本图书馆 CIP 数据核字（2015）第 090557 号

本书版权登记号：图字：01-2013-6572

安全模式最佳实践

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：吴 怡　　责任校对：殷 虹
印　　刷：三河市宏图印务有限公司　　版　　次：2015 年 5 月第 1 版第 1 次印刷
开　　本：186mm × 240mm 1/16　　印　　张：29.5
书　　号：ISBN 978-7-111-50107-7　　定　　价：99.00 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

译 者 序

随着信息技术的飞速发展，互联网日益成为人们生活中不可缺少的一部分，社交网络、微博、移动互联网、云计算、物联网等各种新技术、新应用层出不穷。但不管是 Facebook、Twitter 等新兴互联网公司的迅速崛起，还是 Android 日益成为智能手机市场的主流操作系统，信息安全一直都是永恒的话题。

安全模式是在给定的场景中，为控制、阻止或消减一组特定的威胁而采取的通用解决方案。在信息系统和软件设计中使用安全模式，可以有效地增强信息系统和软件的架构安全性，降低其安全风险。本书系统全面地阐述了安全模式的由来、基本概念、重要作用和主要应用，尤其是详细描述了大量具体安全模式的实例，对信息系统和软件架构设计与分析人员有重要的参考价值。对于每一个安全模式实例，本书均描述其应用场景，并针对应用场景所面临的威胁和亟需解决的问题，提出对应的解决方案（即模式），再通过直观的 UML 图说明模式的具体实现、优点和已知应用。由于作者采用了“提出问题→分析问题→解决问题→总结”的思路，即使读者对安全模式知之甚少，只要有一定的架构设计和信息安全基础，都能很快理解某一安全模式并加以应用。此外，本书内容翔实、图文并茂，非常适合架构设计和分析人员快速掌握安全模式，从本书“按图索骥”。

本书得到国家自然科学基金项目（61100047、61272493）的支持。参与本书翻译的人员有：董国伟、张普含、宋晓龙、刘晓舟、邵帅、王欣、辛伟，在此真诚感谢特约编辑朱筱丹女士，她对本书提出了许多建设性意见，为内容质量的提升付出了大量心血。由于时间和水平有限，书中错漏在所难免，敬请广大读者批评指正。

董国伟

2015 年 2 月

关于作者

Eduardo B. Fernandez（又名 aka Eduardo Fernandez-Buglioni）是美国 Florida Atlantic University 计算机科学与工程系的教授。业余时间，他还是智利 Universidad Tecncia Federio Santa Maria 的客座教授。他在授权访问模型、面向对象分析与设计、安全模式等方面发表了大量的论文，并编撰了四本书籍。他曾多次在全球性质的学术和产业会议上发表演讲，目前主要关注安全模式、网络服务、云计算安全与容错等技术。他在普渡大学获得电气工程理科硕士学位，在加州大学洛杉矶分校获得计算机科学博士学位。他是 IEEE、ACM 会员，同时也是 IBM、Allied Signal、摩托罗拉、朗讯等公司的顾问。他的个人主页是 www.cse.fau.edu/~ed。

关于序作者

Markus Schumacher 自 2006 年起一直担任 Virtual Forge Gmbh 公司的首席执行官，并是该公司的创始人之一。该公司专门从事 SAP 公司应用程序安全性方面的工作。他以前就职于 Fraunhofer Institute for Secure Information Technology (SIT)，并且曾在 SAP 公司担任安全产品经理。他现在关注的领域包括安全开发、安全测试、安全响应、产品认证（通用标准 CC）和开发人员的宣传活动。他曾获得计算机科学博士学位，发表了大量的论文，与人合著了多部书籍，包括《 Secure ABAP Programming 》和《 Security Patterns-Volume 1 》，并且多次在国际会议上发表演讲。

Forword 序

有人认为安全很简单。使用一点点的密码技术，增加一些防火墙和密码——理论上是这样……

我在上世纪 90 年代中期从事安全领域的研究时，遇到了很多自认为能够保证其软件安全的人。他们使用安全措施中的某些要素，以此来解决遇到的任何问题。更加糟糕的是：有时候他们并不使用已经存在的要素，而是使用他们自己创建的——实际上在延续着以前大量项目中存在的相同错误。实践证明他们是错误的：安全从来都不简单——通常都至少有一个漏洞，总有意想不到的问题。如果不够专业，就会忽视一些东西。新闻头条经常披露的安全事件证明我们所学的还远远不够。

应用程序处于不安全状态的主要原因是：

- 缺少时间——归因于紧迫的项目开发截止时间和紧张的预算。
- 缺少知识储备——IT 专家通常都不是安全专家。
- 缺少优先级——通常会优先考虑功能和性能。

这就是我们注定会失败的原因。黑客可以轻松地进入系统，窃取或者修改数据，然后毫无痕迹地离开。有些时候，直到新的设计被竞争对手剽窃，或者本应保密的消费者数据被公布在公共网站上，或者新闻记者报道了一些奇妙的新故事，受害者才知道这些糟糕的事情已经发生。更加糟糕的是，现代应用程序变得越来越复杂，例如目前时髦的移动应用和云计算。边界逐渐消失，已知领域的保护方法也是困难重重。

在传统的工业中，我们拥有发展了数百年的知识。我们知道怎样建造能抵御风、雨、地震的桥梁，知道如何生产在撞击中提供逃生机会的结实的汽车。我们懂得在特定环境下解决问题的方法，这些方法总结出来称为模式。软件工程也已经采用模式有一段时间了。在 20 世纪 90 年代末，安全问题模式的研究出现了一些成果，模式社区不断总结并汇集这些模式，收集如何正确完成模式的安全专业知识，产生了第一个综合性的安全模式集合。

很明显，这项工作并不可能通过出版几本书就完成。除去发掘更多的知识、编写更多的模式外，一个有趣的问题就是怎样有效地应用它们。这两个问题在 Eduardo B. Fernandez（一名计算机科学与安全模式的先驱者）的新书中会有所回答。他一直在研究我们十多年前发起的工作。我非常荣幸能够成为他撰写本书时交流问题的对象。

本书对于那些想要理解如何开发可靠应用程序的软件工程师来说是一个最新的指南，它提供了在日常工作中收集到的安全模式知识。安全并不简单，但是当你理解了具体问题的利益、责任和依赖关系，它就会简单很多。

Markus Schumacher

2013 年 3 月于德国海德堡

Preface 前　言

一个人只有大量地阅读，各处去周游，才能够见多识广。

——米格尔·德·塞万提斯《堂吉诃德》

我在加入 IBM 后，进行了近九年的安全技术工作。在 IBM 工作期间，我与人合著了一本关于数据库安全的书，那是最早关注这方面主题的书籍之一。后来，我意识到大量的安全知识被浪费掉了，因为从业者没有读过此类书籍和论文；他们始终在重复着相同的错误。特别是软件开发者对于安全性知之甚少。再后来，我参加了一个关于模式的会议，意识到将安全知识以模式形式进行陈述将是传播这种知识的有效途径。在那段时间里，Yoder 和 Barcalow[Yod97] 发表了一篇使用模式形式陈述安全方法的论文，这让我更加深信，这是一个好的方向。再再后来，我发现安全模式除了向没有经验的开发者传播安全知识之外，对安全专家也十分有用，可以帮助他们以一种系统级的方法应用安全知识去开发新的应用程序或者产品，理解复杂的标准，审计复杂的应用程序和重新开发遗留系统。于是我与人合著了一本书，该书介绍了 2005 年之前发布的绝大部分安全模式类型。然而，自从那本书出版后，出现了更多的模式。

我已经写了超过 80 个模式，大多数都会在本书中介绍。其他作者也发表了一些模式，完善了本书（参见第 1 章）。我已经在每个模式的“参见”小节中列出了这些补充内容。需要注意的是别人使用的符号或者模式格式可能与我们有所不同。

我不想过度阐述，所以可能会遗漏一些有价值的模式。希望能够在本书英文版的网站：http://www.wiley.com/go/securitypatterns 或者是在新版本中，将那些未来发现的模式不断完善进来，模式可以在使用或者更好地理解之后进行完善。本书中的一部分模式是在 15 年前完成的，而其他的模式仍处于发展阶段。当审视这些相对较早的模式时，我意识到现在可以把它们写得更好一些，这也就延迟了本书的定稿时间。本书不是 2006 年出版的书籍 [Sch06b] 的第二卷或者升级版，而是体现了我这些年的工作成果。为了保证完整性，一些

来自于我的更早书籍的模式也加入本书中；我希望最终能够做出一个完整的目录，虽然现在还没有成功。其他作者也写出了一些好的模式，这样就会有一批高质量的模式供开发者和研究人员使用。我的读者大部分都是希望把安全性整合在产品中的软件开发者，然而，本书也适合研究人员、计算机科学专业的学生和对系统安全感兴趣的人参考。

我们工作中的一个难点就是用了很长的时间来统一图形风格。书中描述的所有模式要么是在模式会议上讨论过，要么是在研究会议上展示过。然而，为了本书的出版，我对它们重新进行了修改，有的部分改动还比较大。我仍然非常积极地接受那些提供最初想法的原始版本，阅读每一行并完善它们的内容。换句话说，本书是我全新的创作，而不仅仅是过去工作的编辑或者我学生作品的展示。

仅有模式还是不够的：我们的最终目标是建立安全的系统。为了这个目标，我一直都在研究使用模式创建安全系统的方法论，本书中也会演示几个例子。严格意义上来说，我使用的方法是一种工程方法。但这不意味着不会谈到理论，但我会尽量只在必要的时候提出理论；同样，也不意味着使用代码：尽管我会给一些代码示例，但大多时候会使用模型进行举例。为了能够支持现在系统的复杂度，我们需要对模型进行抽象。模式的重要作用就是引导我们进行系统级的思考。一个系统不仅仅是它各个部分的组合，因此，单单关注孤立的代码和硬件只是一种微观视角，无法带来安全的系统。

每个模式可以用一页来介绍理念，也可以用 30 页来描述细节，我选择的是一种介于两者之间的中间层次。目标是让读者通过足够的细节描述理解模式的意义，并且评估它们的可行性。我发现这种层次的细节描述在我的工作中最为有效。我已经忍住了添加安全背景相关资料的冲动：这些已经在好几本书中进行过介绍（见第 1 章）。

因为我在大学里工作，所以被多次指责“不注重实践性”。其实我在企业里工作了十年左右，并且为很多公司做过顾问，所以有一些产业界的经验。当我编写这些模式时，我的那些已经在企业界工作的学生也提供了一些重要的产业视角。在某种程度上，本书是一本跨学科的书籍，将安全性与软件体系结构联系起来了[⊖]。

我很希望听到对本书的建议和批评意见。虽然这些模式包括了计算机系统体系结构的所有范围，但我也确信在某些方面我的理解并不正确。我对安全模式在实际项目中的使用特别感兴趣。如果有任何建议，请发送邮件给我：ed@cse.fau.edu。Markus Schumacher 和我会在 securitypatterns.org 上发布有关模式的评论。

⊖ 本书的确与软件体系结构紧密相连，推荐阅读《现代操作系统》第三版第 9 章“安全”。——译者注

本书结构

本书分为三部分。第一部分描述使用模式的动机、经验，以及本书的目标，并且展示了作者的安全开发方法论。第二部分是安全模式的详细介绍，包括计算机系统不同体系结构层次的模式。第三部分展示了一些模式的应用、模式表，并且指出了今后可能的研究方向。

致谢

本书是我在安全方面研究多年的成果。在这个过程中，我参加了多个安全模式会议，与全球各地从事这项工作的同行进行交流，倾听他们的意见，他们均对本书的完成做出了贡献。特别要感谢的是我的学生们，尤其是 Nelly Delessy、Keiko Hashizume、Ola Ajaj、Juan C. Pelaez 和 Ajoy Kumar，他们撰写了这些模式中的几个版本。我的同事 Maria M. Larrondo-Petrie 和 Mike Van Hilst 与我协作发布了一些模式。我还有如下一些国际合作者：Nobukazu Yoshioka 和 Hironori Washizaki (Japan)、Günther Pernul (German)、David LaRed (Argentina)、Anton Uzunow (Australia)、Fabricio Braz (Brazil)、Jaime Muñoz Arteaga (Mexico) 和 Antonio Maña (Spain)。

模式语言会议（PLoP、EUROPLoP、AsianOLOP 和 LatinAmerican PLOP）的指导专家和研讨会参与人员都给予了非常有价值的建议，特别是 Joe Yoder、Fabio Kon、Richard Gabriel、Rosana Braga、Ralph Johnson、Lior Schachtert 等。Craig Heath 进行了前三章的注释工作。

Wiley 英国出版社的编辑人员 Ellie Scott、Birgit Gruber 和 Sara Shlaer，以及 WordMongers 的 Steve Rickaby，都给予了非常多的帮助和支持。Markus Schumacher 是一个非常称职的指导者，他能够找到严重的错误和遗漏的内容。在这里，我向他们表示诚挚的感谢！

推荐阅读

网站安全攻防秘笈：防御黑客和保护用户的100条超级策略

作者：（美）Ryan C. Barnett ISBN：978-7-111-47803-4 定价：79.00元

渗透测试实践指南：必知必会的工具与方法（原书第2版）

作者：（美）Patrick Engebretson ISBN：978-7-111-47344-2 定价：59.00元

Kali渗透测试技术实战

作者：（美）James Broad 等 ISBN：978-7-111-47320-6 定价：59.00元

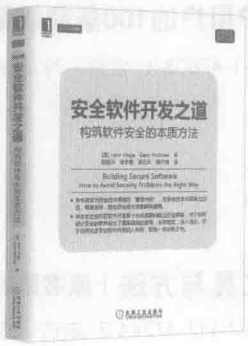
Web应用漏洞侦测与防御：揭秘鲜为人知的攻击手段和防御技术

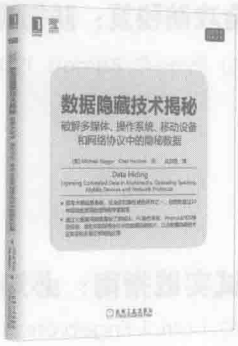
作者：（美）Mike Shema ISBN：978-7-111-47253-7 定价：69.00元

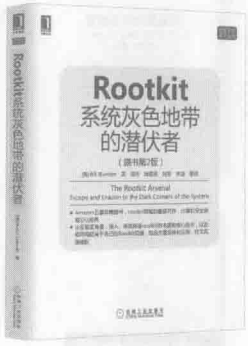
Metasploit渗透测试魔鬼训练营

作者：诸葛建伟 等 ISBN：978-7-111-43499-3 定价：89.00元

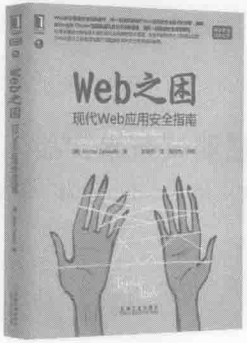
推荐阅读

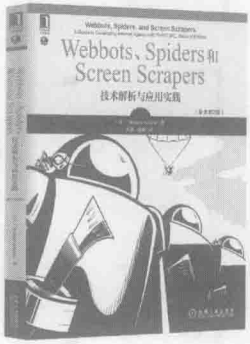

安全软件开发之道
构筑软件安全的本质方法
Building Secure Software
How to Avoid Security Problems the Right Way

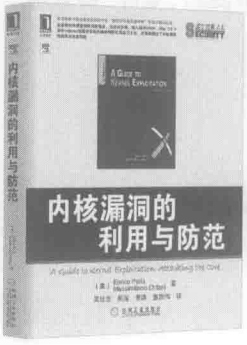

数据隐藏技术揭秘
破解多媒体、操作系统、移动设备和网络协议中的隐秘数据
Data Hiding

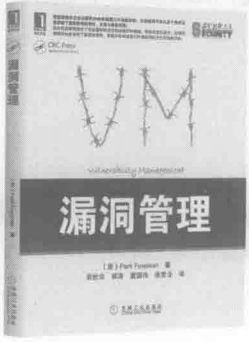

Rootkit
系统灰色地带的潜伏者
（跨书版2版）
The Rootkit Arsenal

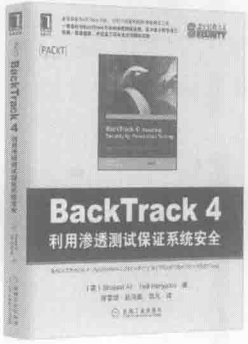

恶意软件、Rootkit和僵尸网络
Malware, Rootkits & Botnets
A Beginner's Guide


Web之困
现代Web应用安全指南


Webbots, Spiders, and Screen Scrapers
Webbots、Spiders和Screen Scrapers
技术解析与应用实践


内核漏洞的利用与防范
A Guide to Kernel Exploitation


漏洞管理
Vulnerability Management


BackTrack 4
利用渗透测试保证系统安全

目 录 *Contents*

第二部分 模 式