
/THEORY/IN/PRACTICE
安全之美
Beautiful Security
分享卓越安全专家的思考
O'REILLY®
机械工业出版社
China Machine Press
HZ BOOKS
华章科技
Andy Oram & John Viega 编
徐波 沈晓斌 译

安全之美

O'REILLY®

Beijing · Cambridge · Farnham · Köln · Sebastopol · Tokyo

O'Reilly Media, Inc. 授权机械工业出版社出版

机械工业出版社

图书在版编目（CIP）数据

安全之美 /（美）奥拉姆（Oram, A.）等编；徐波，沈晓斌译．—北京：机械工业出版社，2011.4
（O'Reilly精品图书系列）
书名原文：Beautiful Security

ISBN 978-7-111-33477-4

Ⅰ.安… Ⅱ.①奥… ②徐… ③沈… Ⅲ.信息系统—安全技术 Ⅳ.TP309

中国版本图书馆CIP数据核字（2011）第024885号

北京市版权局著作权合同登记

图字：01-2009-3521

书　　名 / 安全之美
书　　号 / ISBN 978-7-111-33477-4
责任编辑 / 秦健
封面设计 / Mark Paglietti，张健
出版发行 / 机械工业出版社
地　　址 / 北京市西城区百万庄大街22号（邮政编码　100037）
印　　刷 / 北京京师印务有限公司
开　　本 / 178毫米×233毫米　16开本　17.25印张
版　　次 / 2011年4月第1版第1次印刷
定　　价 / 65.00元（册）

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) 88378991，88361066
购书热线：(010) 68326294，88379649，68995259
投稿热线：(010) 88379604
读者信箱：hzjsj@hzbook.com

O'Reilly Media, Inc.介绍

为了满足读者对网络和软件技术知识的迫切需求，世界著名计算机图书出版机构O'Reilly Media, Inc. 授权机械工业出版社，翻译出版一批该公司久负盛名的英文经典技术专著。

O'Reilly Media, Inc. 是世界上在UNIX、X、Internet和其他开放系统图书领域具有领导地位的出版公司，同时也是联机出版的先锋。

从最畅销的《The Whole Internet User's Guide & Catalog》（被纽约公共图书馆评为20世纪最重要的50本书之一）到GNN（最早的Internet门户和商业网站），再到WebSite（第一个桌面PC的Web服务器软件），O'Reilly Media, Inc. 一直处于Internet发展的最前沿。

许多书店的反馈表明，O'Reilly Media, Inc.是最稳定的计算机图书出版商——每一本书都一版再版。与大多数计算机图书出版商相比，O'Reilly Media, Inc. 具有深厚的计算机专业背景，这使得O'Reilly Media, Inc. 形成了一个非常不同于其他出版商的出版方针。O'Reilly Media, Inc. 所有的编辑人员以前都是程序员，或者是顶尖级的技术专家。O'Reilly Media, Inc. 还有许多固定的作者群体——他们本身是相关领域的技术专家、咨询专家，而现在编写著作，O'Reilly Media, Inc. 依靠他们及时地推出图书。因为O'Reilly Media, Inc. 紧密地与计算机业界联系着，所以O'Reilly Media, Inc. 知道市场上真正需要什么图书。

译者序

从20世纪末以来，Internet得到了极为迅猛的发展，仅用了十年左右的时间就在全球范围内普及。Internt已经融入绝大多数公司、家庭和个人的工作生活之中。我们可以真真切切地感受到层出不穷的新技术给我们的生活所带来的便捷。我们可以足不出户在网上订购自己喜欢的商品。在车站、机场等候时，我们不必像以前那样靠翻报纸来打发时间，而是可以通过无线上网，漫游精彩的网络世界。我们不必再为无法看到心爱的球队比赛而发愁，丰富的网络直播资源可以帮助我们解决这个烦恼。总之，Internet彻底改变了我们的生活方式，使我们的生活变得更加精彩。

但是，鲜花的后面往往可能就是陷阱。从Internet诞生之日起，网络安全就一直是个引人关注的话题。从历史悠久的病毒、木马到最新的网络诈骗，网络安全威胁一直是一把悬在Internet头上的达摩克利斯之剑。由于网络安全威胁的主流逐渐从单纯以破坏为主的病毒、木马转向以获取经济利益为目标的网络诈骗，因此它的危害也越来越大。近些年来，网络上所出现的网络诈骗案件越来越多，很多网友由于对假冒的网络购买链接警惕性不足而蒙受了经济损失。随着网络越来越广泛地渗透到人们的日常生活中，对网络安全的防范也必将越来越引起人们的重视。

本书萃取了十余位闻名瑕迩的安全专家的智慧，如Philip Zimmermann、Anton Chuvakin、Peiter“Mudge”Zatko等。有些专家着眼于网络安全威胁的心理因素，有些专家侧重于对安全度量指标的讨论，有些专家对电子商务中的网络支付平台的弱点进行了分析，有些专家则对近些年来所发生的几个重大网络犯罪事件进行了详尽分析，还有一些专家对未来的网络安全进行了展望。这些专家的论著对于网络安全从业人员的工作有着非常好的指导意义。对于关注网络安全的人们，这些文章能够极大地拓宽他们的视野，使他们能够发现网络安全的新天地。

本书的翻译工作主要由徐波、沈晓斌完成。另外，姚雪存、陈永军、李福军、杨洁、应巧敏、张瑜等人也为本书的翻译工作作出了贡献。

前言

如果有人相信新闻标题可以揭示趋势，那么对于计算机安全领域而言现在是个有趣的时刻。当本书出版时，我阅读了一个能够打开麦克风和摄像头并窃取数据的软件的部分代码。这个软件在103个国家的超过1200台计算机上安装，尤其是在大使馆和其他敏感的政府部门。另外，一家法庭支持美国调查官在没有得到授权的情况下可以查看电话和Internet记录（只要交谈的另一端是在美国境外）。最新公布的漏洞包括Adobe Acrobat和Adobe Reader的一个缓冲区溢出漏洞（当前常称为漏洞攻击，英文为exploit），允许攻击者在用户打开PDF之后在用户的系统中通过用户的权限执行任意代码。

新闻标题实际上并不能很好地提示趋势，因为在漫长的历史中，它是由微妙的革命性变化所驱动的，而这种变化往往只有少数人注意到，例如编写本书的前沿安全专家们。读者可以在本书中发现安全威胁的发展方向以及针对它们的响应。

我在第一段中所提到的所有令人惊恐的新闻对于安全领域而言只是普通的业务而已。是的，它们正是我们应该担忧的安全趋势的一部分，但我们还需要注意更新的、更不易被觉察的漏洞。本书的作者们数十年来一直奋斗在第一线，努力发现我们的工作习惯中的脆弱环节，并提议用非常规的方式来处理它们。

为什么安全是美丽的

我要求安全专家John Viega想方设法为本书寻找一些作者，以便向普通计算机用户提供一些与安全有关的观点。除了在媒体上所看到的骇人听闻的关于网络入侵和盗窃的新闻之外，普通人一般都觉得安全是一件乏味的事情。

对许多人而言，安全就是系统管理员喋喋不休地提醒他们创建备份文件夹，无穷无尽的在网页显示之前跳出来的要求输入密码的对话框。办公室职员每次抄读办公桌边的笔记本上所记录的密码时都怒目圆睁小声咒骂（笔记本就放在打印出来的预算材料的上面，事实上办公室管理人员要求应该将它锁在抽屉里面）。如果这就是安全，那还会有谁想从事这个职业呢？谁会从O'Reilly购买一本关于安全的书呢？谁会一次花费半分钟以上的时间去思考安全呢？

对于那些肩负创建安全系统任务的人们，他们所付出的努力看上去是毫无希望的。站在旁边的人不会对他们的工作提供任何协助，业务经理也拒绝在安全上多花一分钱。程序员和系统管理员由于他们必须使用的工具和语言存在没完没了的零日攻击和未打补丁的漏洞也逐渐变得懒散起来。

这就是为什么关于安全的书卖得很差（尽管在过去的一两年里销量有所上扬）。关于如何入侵系统的书要比关于如何保护系统的书好卖得多，这个趋势着实令我震惊。

是的，本书应该改变这个现象。它应该向读者展示安全是一项最为激动人心的职业。它并不枯燥，也没有太多的官僚主义，更没有太多的约束。事实上，它和其他技术一样充满着想象力。

多年以来，我编辑过的大多数编程书籍都提供了关于安全的内容。这样的内容当然是非常实用的，因为它们允许作者讲述一些基本原则和一些良好习惯。但是，我已经对这种做法感到厌烦，因为它为安全话题划了一条分界线。它所灌输的都是一些老生常谈的安全观点，是一些锦上添花或者事后诸葛亮的东西。本书将颠覆这些观念。

John为本书选择了一些作者，他们已经在安全领域证明了自己具有独特的观点，并且有一些新的思路要和大家分享。有些作者设计了数以千计的人所依赖的系统，有些作者在大型公司担任高管职位，有些作者曾为法庭作证并为政府部门工作。所有的作者都在寻找普通人所不知道的问题和解决方案，但是这可能需要几年的时间才会收到成效。

本书的作者指出：有效的安全需要你始终保持警惕。它会打破技术、认知和组织结构的边界。安全界的黑帽们千方百计通过创新来取得成功。因此，负责防御他们的人们同样需要创新。

本书的作者肩负着世界范围内的信息安全使命，让他们抽出时间编写本书是一件很困难的事。事实上，许多作者在平衡本职工作和本书的写作任务时感受到了压力。但是，他们所花的时间是值得的，因为本书将会促进他们实现更远大的目标。如果有更多的人对安全领域产生兴趣，决定进一步对它进行探索，并向尝试通过组织上的变化以实现更好保护的人们给予他们的关注和支持，这本书就值得作者所付出的心血。

2009年3月19日，美国参议院商业、科学和交通委员会举行了一个听证会，它的主题是

信息技术专家的缺乏以及这种现象对美国的网络安全的危害。让学生和专业人员对安全问题产生兴趣是一项极为迫切的需求，本书就代表了迈向这个目标的一小步。

本书的读者

本书适用于那些对计算机技术感兴趣并希望在最尖端领域体验生活的人们。本书的读者包括可能追求职业生涯的学生、具有一定编程背景的人们以及对计算机有着适度或深入了解的人们。

本书的作者在解释技术时尽量放低门槛，使相对新手级的读者也能领略到攻击和防御活动方式的感觉。专家级的读者能够更多地享受讨论的乐趣，因为本书能够加深他们对安全原则的理解，并提供了未来研究的指导方针。

捐赠

本书的作者们向互联网工程任务组（The Internet Engineering Task Force，IETF）捐赠本书的版税。这个组织对于*Internet*以及其具有远见的自我管理式的迷人模型的发展极为关键。如果没有IETF具有奉献精神的成员们的科学讨论、灵活的标准制定和明智的妥协，Internet的发展是无法想象的。IETF在自己的网页上把自己描述成“由网络设计者、操作者、生产商和研究人员所组成的大型开放式国际社区”。O'Reilly将把版税汇给互联网社会（The Internet Society，ISOC），该组织长期向IETF提供资金和有组织的支持。

材料的组织

本书内容并没有按任何特定的方案进行排列，但还是经过了整理，以便提供引人入胜的阅读体验，方便读者惊喜地发现新观点。不过，还是将那些讲述相似主题的内容放在了一起。

第1章　心理上的安全陷阱　作者Peiter“Mudge”Zatko

第2章　无线网络：社会工程的沃土　作者Jim Stickley

第3章　美丽的安全度量指标　作者Elizabeth A. Nichols

第4章　安全漏洞的地下经济　作者Chenxi Wang

第5章　美丽的交易：重新思考电子商务的安全　作者Ed Bellis

第6章　捍卫在线广告：新狂野西部的盗匪和警察　作者Benjamin Edelman

第7章　PGP信任网络的演变　作者Phil Zimmermann和Jon Callas

第8章　开源Honeyclient：先发制人的客户端漏洞检测　作者Kathy Wang

第9章　未来的安全齿轮和杠杆　作者Mark Curphey

第10章　安全设计　作者John McManus

第11章　促使公司思考：未来的软件安全吗　作者Jim Routh

第12章　信息安全律师来了　作者Randy V. Sabett

第13章　美丽的日志处理　作者Anton Chuvakin

第14章　事件检测：寻找剩余的68%　作者Grant Geyer和Brian Dunphy

第15章　无需真实数据就能出色完成工作　作者Peter Wayner

第16章　铸造新词：PC安全剧场　作者Michael Wood和Fernando Francisco

使用本书的代码示例

本书是为了帮助你完成工作。通常来说，你可以在你的程序和文档中使用本书的代码。除非你使用了本书的大量代码，否则你无需获取我们的许可。例如，写一个程序用到本书的几段代码不需要获得许可；销售和分发O'Reilly 丛书的代码需要获得许可；引用本书的样例代码来解决一个问题不需要获得许可；使用本书的大量代码到你的产品文档中需要获得许可。

我们不要求你（引用本书时）给出出处，但是如果你这么做，我们对此表示感谢。出处通常包含标题、作者、出版社和 ISBN。例如："*Beautiful Security*, edited by Andy Oram and John Viega. Copyright 2009 O'Reilly Media, Inc., 978-0-596-52748-8"。

如果你觉得你对本书样例代码的使用超出了这里给出的许可范围，请和我们联系：*permissions@oreilly.com*。

如何联系我们

请把对本书的评论和问题发给出版社：

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

O'Reilly的每一本书都有专属网页，你可以在那儿找到关于本书的相关信息，包括勘误表、示例代码以及其他的信息。本书的网站地址是：

http://www.oreilly.com/catalog/9780596527488/

对于本书的评论和技术性的问题，请发送电子邮件到：

bookquestions@oreilly.com

关于本书的更多信息、会议、资料中心和网站，请访问以下网站：

http://www.oreilly.com

目录

前言

第1章 心理上的安全陷阱 ……1

Peiter "Mudge" Zatko

1.1 习得性无助和无从选择 ……2

1.1.1 实例：Microsoft是如何允许L0phtCrack的 ……3

1.1.2 密码和身份认证可以从一开始就做得更好 ……6

1.1.3 客户的习得性无助——无从选择 ……8

1.2 确认陷阱 ……9

1.2.1 概念简介 ……10

1.2.2 分析师确认陷阱 ……11

1.2.3 陈腐的威胁模型 ……11

1.2.4 正确理解功能 ……12

1.3 功能锁定 ……13

1.3.1 安全位置的潜在风险 ……14

1.3.2 降低成本与未来收益：ISP实例 ……15

1.3.3 降低成本与未来收益：能源实例 ……16

1.4 小结 ……19

第2章 无线网络：社会工程的沃土 ……21

Jim Stickley

2.1 轻松赚钱 ……22

2.1.1 设置攻击 ……23

2.1.2 隐私的聚宝盆 ……24

2.1.3 Web安全的基本缺陷：不要相信可信系统 ……25

2.1.4 建立无线信任 ……25

2.1.5 采用可靠的解决方案 ……26

2.2 无线也疯狂 ……27

2.2.1 无线侧信道 ……28

2.2.2 无线接入点自身如何 ……30

2.3 无线仍然是未来 ……30

第3章 美丽的安全度量指标 ……31

Elizabeth A. Nichols

3.1 安全度量指标的类比：健康 ……32

3.1.1 不合理的期待 ……33

3.1.2 数据透明性 ……33

3.1.3 合理的度量指标 ……34

3.2 安全度量指标的实例 ……36

3.2.1 巴林银行：内部侵害 ……36

3.2.2 TJX：外部侵害 ……46

3.2.3 其他公共数据来源 ……56

3.3 小结 ……57

第4章 安全漏洞的地下经济 ……59

Chenxi Wang

4.1 地下网络的组成和基础设施 ……60

4.1.1 地下通信基础设施 ……61

4.1.2 攻击基础设施 ……61

4.2 回报 ……62

4.2.1 数据交换 ……62

4.2.2 信息来源 ……63

4.2.3 攻击向量 ……64

4.2.4 洗钱游戏 ……66

4.3 如何对抗日益增长的地下网络经济 ……66

4.3.1 降低数据的价值 ……67

4.3.2 信息的权限分离 ……67

4.3.3 构建动力/回报结构 ……67

4.3.4 为数据责任建立评估和声誉体系 ……67

4.4 小结 ……68

第5章 美丽的交易：重新思考电子商务的安全 ……69

Ed Bellis

5.1 解构商业 ……70

分析安全环境 ……71

5.2 微弱的改良尝试 ……71
5.2.1 3D安全 ……72
5.2.2 安全电子交易 ……74
5.2.3 单用途和多用途虚拟卡 ……75
5.2.4 破灭的动机 ……75
5.3 重塑电子商务：新的安全模型 ……78
5.3.1 需求1：消费者必须通过认证 ……78
5.3.2 需求2：商家必须通过认证 ……79
5.3.3 需求3：交易必须经过授权 ……79
5.3.4 需求4：认证数据不应被认证方和被认证方之外的其他各方所共享 ……79
5.3.5 需求5：过程不能完全依赖共享秘密 ……80
5.3.6 需求6：认证应该是可移植的（不受硬件或协议所限） ……80
5.3.7 需求7：数据和交易的机密性和完整性必须得到维护 ……80
5.4 新模型 ……80

第6章 捍卫在线广告：新狂野西部的盗匪和警察 ……83

Benjamin Edelman

6.1 对用户的攻击 ……83
6.1.1 充满漏洞的横幅广告 ……83
6.1.2 恶意链接广告 ……86
6.1.3 欺骗式广告 ……88
6.2 广告客户也是受害者 ……91
6.2.1 虚假的印象 ……92
6.2.2 避开容易受骗的CPM广告 ……93
6.2.3 广告客户为何不奋起反击 ……97
6.2.4 其他采购环境的教训：在线采购的特殊挑战 ……98
6.3 创建在线广告的责任制 ……98

第7章 PGP信任网络的演变 ……99

*Phil Zimmermann*和*Jon Callas*

7.1 PGP和OpenPGP ……99
7.2 信任、验证和授权 ……100

7.2.1 直接信任 ……101
7.2.2 层次式信任 ……101
7.2.3 累积式信任 ……102
7.2.4 基本的PGP信任网络 ……104
7.2.5 最早的信任网络的毛边 ……106
7.3 PGP和加密的历史 ……108
7.3.1 早期的PGP ……108
7.3.2 专利和输出问题 ……109
7.3.3 密码战争 ……110
7.3.4 从PGP 3到OpenPGP ……111
7.4 对最初信任网络的改进 ……111
7.4.1 撤销 ……111
7.4.2 伸缩性问题 ……114
7.4.3 签名的膨胀和困扰 ……115
7.4.4 证书内偏好 ……117
7.4.5 PGP全球目录 ……118
7.4.6 可变信任评分 ……119
7.5 未来研究的有趣领域 ……119
7.5.1 超级合法 ……119
7.5.2 社交网络和流量分析 ……119
7.6 参考资料 ……120

第8章 开源Honeyclient：先发制人的客户端漏洞检测 123

Kathy Wang

8.1 进入Honeyclient ……124
8.2 世界上第一个开源Honeyclient简介 ……125
8.3 第二代Honeyclient ……127
8.4 Honeyclient的操作结果 ……130
8.4.1 Windows XP的透明活动 ……130
8.4.2 Honeyclient数据的存储和关联 ……131
8.5 漏洞攻击的分析 ……132
8.6 当前Honeyclient实现的限制 ……134
8.7 相关的工作 ……135
8.8 Honeyclient的未来 ……137

第9章 未来的安全齿轮和杠杆 ……139
Mark Curphey
9.1 云计算和Web服务：这里是单机 ……141
9.1.1 创建者和破坏者 ……142
9.1.2 云计算和Web服务是拯救方案 ……144
9.1.3 新曙光 ……145
9.2 结合人、流程和技术：业务流程管理的潜力 ……146
9.2.1 发散型世界的发散型安全 ……146
9.2.2 BPM作为多站点安全的指导方针 ……147
9.3 社交网络：当人们开始通信时，大变革发生了 ……149
9.3.1 社交网络的艺术状态和潜力 ……150
9.3.2 安全行业的社交网络 ……151
9.3.3 数字中的安全 ……152
9.4 信息安全经济：超级数据解析和网络新规则 ……153
9.5 长尾变型的平台：未来为什么会截然不同 ……156
9.5.1 生产工具的大众化 ……156
9.5.2 发行渠道的大众化 ……157
9.5.3 连接供应和需求 ……158
9.6 小结 ……158
9.7 致谢 ……159
第10章 安全设计 ……161
John McManus
10.1 无意义的指标 ……162
10.2 市场还是质量 ……164
10.3 符合准则的系统开发周期的作用 ……168
10.4 结论：安全之美是系统之美的象征 ……170
第11章 促使公司思考：未来的软件安全吗 ……173
Jim Routh
11.1 隐式的需求也可能非常强大 ……173
11.2 公司为什么需要安全的软件 ……175
11.2.1 如何制订安全计划 ……176
11.2.2 修正问题 ……178
11.2.3 把安全计划扩展到外包 ……179

11.3 对现有的软件进行安全化……180
11.4 分析：如何使世界上的软件更安全 ……182
11.4.1 最好的软件开发人员创建了具有漏洞的代码…182
11.4.2 Microsoft领先一步……183
11.4.3 软件开发商给了我们想要的，却不是我们需要的 ……184

第12章 信息安全律师来了……187

Randy V. Sabett

12.1 文化……188
12.2 平衡……190
12.2.1 数字签名指南 ……190
12.2.2 加利福尼亚数据隐私法 ……191
12.2.3 安全的投资回报率……192
12.3 通信……194
12.3.1 技术狂为何需要律师……194
12.3.2 来自顶层的推动力，通过合作实现 ……197
12.3.3 数据泄露小虎队 ……197
12.4 正确做事……198

第13章 美丽的日志处理……199

Anton Chuvakin

13.1 安全法律和标准中的日志……199
13.2 聚焦日志……200
13.3 什么时候日志是极为珍贵的……201
13.4 日志所面临的困难 ……202
13.5 案例研究：瘫痪服务器的背后……204
13.5.1 事故的架构和环境……204
13.5.2 被观察的事件 ……204
13.5.3 调查开始 ……204
13.5.4 使数据起死回生 ……206
13.5.5 小结 ……207
13.6 未来的日志 ……207
13.6.1 来源的扩大化 ……207
13.6.2 未来的日志分析和管理工具 ……208

13.7 结论……209

第14章 事件检测：寻找剩余的68%……211

Grant Geyer和Brian Dunphy

14.1 一个常见起点……212
14.2 改进与上下文相关的检测……213
14.2.1 用流量分析提高覆盖率……214
14.2.2 对监测列表进行综合分析……216
14.3 使用主机日志增强洞察力……217
创建富有弹性的检测模型……218
14.4 小结……222

第15章 无需真实数据就能出色完成工作……225

Peter Wayner

15.1 数据半透明化的工作原理……226
15.2 一个现实的例子……228
15.3 为便利而存储的个人数据……230
15.4 如何权衡……230
15.5 进一步深入……231
15.6 参考资料……232

第16章 铸造新词：PC安全剧场……233

Michael Wood和Fernando Francisco

16.1 攻击不断增加，防御不断倒退……234
16.1.1 在Internet的传送带上……234
16.1.2 不正当行为的回报……235
16.1.3 暴徒的响应……236
16.2 揭穿假象……237
16.2.1 严格审查：传统的和更新的反病毒扫描……237
16.2.2 沙盒和虚拟化：新的银弹……240
16.3 桌面安全的更佳实践……242
16.4 小结……243

附录 作者简介……245