Broadview
www.broadview.com.cn

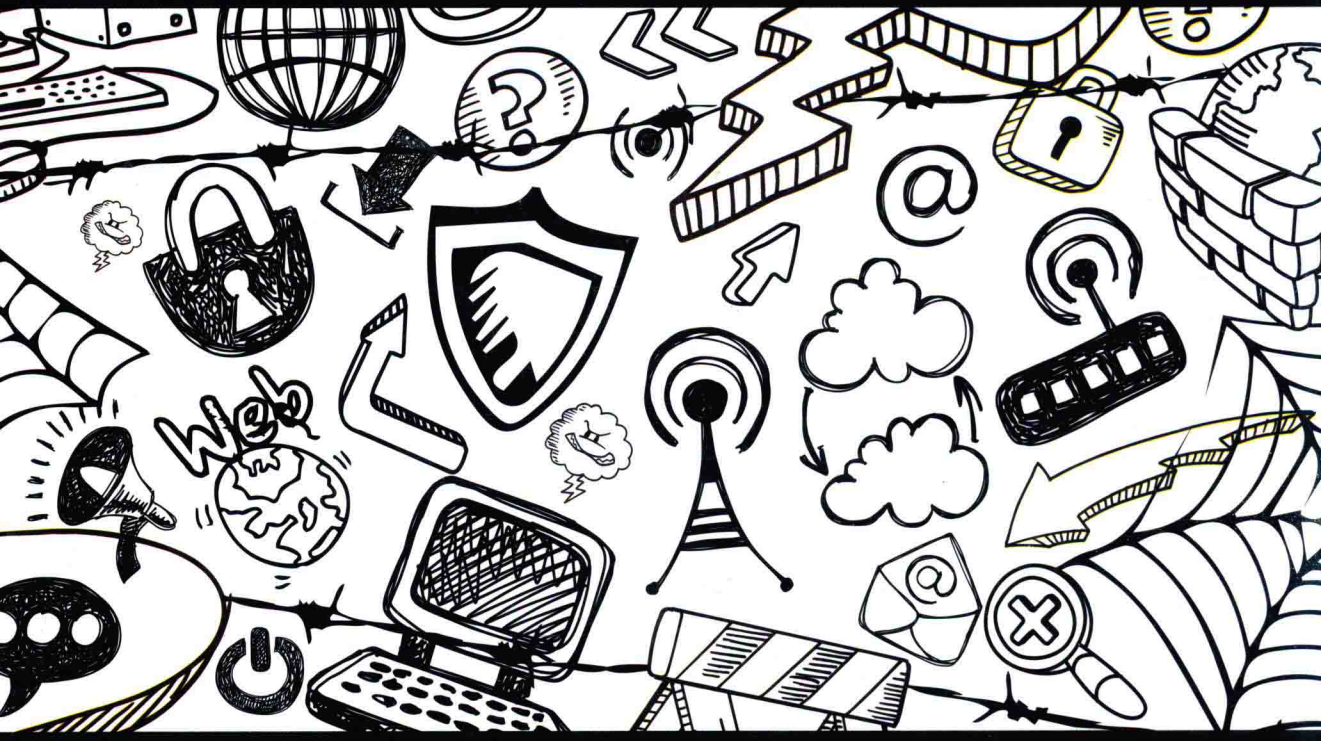
安全技术大系

Pearson

提高系统被渗透的代价，让攻击者知难而退

阻击黑客

技术、策略与案例



Thinking **Security**

Stopping Next Year's Hackers

[美]Steven M. Bellovin 著

徐菲 熊刚 李镇 译

中国工信出版集团

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

安全技术大系

阻击黑客
技术、策略与案例

阜阳师范学院图书馆
藏书

Thinking Security
Stopping Next Year's Hackers

[美]Steven M. Bellovin 著
徐菲 熊刚 李镇 译

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

作者是世界上最受尊重和认可的安全专家之一，他在本书中提供了一种看安全的新视角。

本书第 1 部分从问题定义开始，从系统化的角度看待安全，讨论当前安全发展的变化、安全的思维方式、目标，并且分析了不同的威胁模型。在此基础之上，第 2 部分介绍安全相关的技术，除了对技术本身进行介绍之外，作者还很好地考虑了不同情况、不同需求，以及在应对不同威胁模型时，各种技术的优势和可能面临的问题。第 3 部分介绍具体的安全操作，即如何创建安全的系统，考虑了包括代码、设计、架构、管理以及人员等众多综合因素。第 4 部分分析具体案例，并且对未来的技术发展和应对给出了建议。

本书基于作者在安全领域多年的实际经验，结合新技术的发展，给出了实用而全面的安全技术指导，为创建安全系统提供了很好的借鉴。

Authorized translation from the English language edition, entitled Thinking Security: Stopping Next Year's Hackers, 978-0134277547, by Steven M. Bellovin, published by Pearson Education, Inc., publishing as Addison-Wesley Professional, Copyright © 2016 Pearson Education, Inc.

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from Pearson Education, Inc.

CHINESE SIMPLIFIED language edition published by PEARSON EDUCATION ASIA LTD., and PUBLISHING HOUSE OF ELECTRONICS INDUSTRY Copyright © 2017.

本书简体中文版专有出版权由 Pearson Education 培生教育出版亚洲有限公司授予电子工业出版社。未经出版者预先书面许可，不得以任何方式复制或抄袭本书的任何部分。

本书简体中文版贴有 Pearson Education 培生教育出版集团激光防伪标签，无标签者不得销售。

版权贸易合同登记号图字：01-2016-0604

图书在版编目（CIP）数据

阻击黑客：技术、策略与案例 /（美）斯蒂夫 • M • 贝劳文（Steven M. Bellovin）著；徐菲，熊刚，李镇译. —北京：电子工业出版社，2017.3
（安全技术大系）
书名原文：Thinking Security: Stopping Next Year's Hackers
ISBN 978-7-121-31066-9

Ⅰ. ①阻… Ⅱ. ①斯… ②徐… ③熊… ④李… Ⅲ.①黑客－网络防御 Ⅳ. ①TP393.081

中国版本图书馆 CIP 数据核字（2017）第 047557 号

责任编辑：徐津平
印　　刷：北京中新伟业印刷有限公司
装　　订：北京中新伟业印刷有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编：100036
开　　本：787×980　1/16　印张：22.25　字数：410 千字
版　　次：2017 年 3 月第 1 版
印　　次：2017 年 3 月第 1 次印刷
定　　价：79.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：（010）51260888-819，faq@phei.com.cn。

献给 Diane，千言万语。献给 Rebeca 和 Daniel，

你们让我不要再写书了，但因为你们已经不住在家里了，因此没有投票权。

序言

多数计算机安全类书籍只告诉大家应当做什么和不应当做什么。而本书将会告诉你为什么。

要保证安全，需要做的事情有很多：运行杀毒软件，安装防火墙，将所有东西上锁，遵循严格的检查规定，加密并监视网络中的所有流量，重金聘请安全顾问，等等。可结果却是相当让人失望的：公司在安全上投入巨大，却还是会遭受大量的计算机相关的攻击。很明显，这里还存在问题。

问题的根源具有两面性：我们在保护（以及在保护上投资）错误的东西，我们在这个过程中影响了生产效率。与汽车的车锁不同，有了汽车车锁就能够将车停在不安全的地方，从而加强了汽车的使用功能。而计算机安全似乎是在限制用户做事情，而不是让用户能够在不安全的地方做事情。人们——尤其是雇员——希望能够提高生产效率，当安全措施影响生产效率时，猜测一下什么会被牺牲掉？没错，就是安全。

解决方法同样也有两面性：保护正确的事情，并且让雇员能够很容易地做正确的事情。这不仅仅需要一个列表，还需要对于实际威胁和技术的了解。这就是这本书的内容，如何来思考安全。

保护正确的事情

安全始于知道保护什么，以及保护其不受何种威胁。这也就意味着，任何安全建议，如果没有以这两个问题开始，都是没有意义的。你将会花太多精力在错误的事情上面。如果你是在保护国家的安全机密信息不受外国情报机构的探测，可能就需要应用所有现有的

此为试读，需要完整PDF请访问：www.ertongbook.com

防护方法，以及一些还未出现的防护措施。此外，你还需要保护其不受“3B”的威胁，“3B”即盗窃（Burglary）、贿赂（Bribery）和勒索（Blackmail）。

大多数人都不像对手那样有一些间谍（尽管新闻报道称情况正在改变[Barrett 2015]）。当今的典型黑客都是受利益驱使的，需要问的问题是，黑客是如何利用你的计算机和网络来获益的。如果你在银行工作，那么答案就很明显；用大家都知道的话说，因为银行是钱在的地方。但是坏人可以利用任何一台计算机来盗窃我们个人的东西，因此我们不能放松防御。这些攻击更多可能是随机的，而不是针对特定目标的。即使这样，风险程度也可以划分为不同等级。

这就造成一个结果，防御也是利益相关的。花费比原物价值更多的费用来保护原物是没有意义的。一种值得记住的说法是[Schiffman 2007]“业余人士担心算法，专业人士担心经济”。你的目标并不是让一个系统无法被渗透，而是提高被渗透的代价，让敌人不愿付出高额代价去做，同时降低自己的投入。

我们以典型的密码为例。30 多年来，一直有人不断地告诉我们弱密码是不安全的[Morris and Thompson 1979]。毫无疑问这是正确的，由于弱密码造成的安全问题十分常见。也有人不断告诉我们不应当把密码记下来。但是，自从 1979 年以来，世界在各个方面都有了很大的变化。

假如我设置了一个很强的密码，并且我不只是设置了一个很强的密码，而是对于需要登录的不同网站，设置了很多个不同的强密码。我不可能记住所有的密码，一定会忘掉几个，因此我必须采取密码恢复机制。什么是密码恢复机制呢？对于很多网站来说，它们会把新密码通过邮件发送给我。那么我的账号安全就取决于邮箱的安全了，对吗？不仅如此，还存在一些其他的问题。

对很多人来说，真正的威胁不是密码猜测，而是按键记录器。也就是说，有人在计算机上安装了一些恶意软件。这些软件记录了键盘按键的所有行为，包括密码。即使你设置了一个很强的密码，也记住了这个密码，但只要你通过键盘输入这个密码，那么你的账户就可能被攻破[D. Florêncio, Herley, andCoskun 2007]。与之对应，如果密码是通过一个恢复邮件发送给你，你使用了复制粘贴输入，而不是键盘输入，那么你就会更安全。很多人的邮箱密码都是自动保存的，同样不需要用键盘输入。但是如果用键盘输入了邮箱密码，那么所有的对于网站的密码加强机制都会失效，因为坏人会通过盗用邮箱密码来恢复所有网站的密码。

因此，密码安全问题远比一个简单的检查表更加复杂。你必须要有很强的密码，必须用正确的方式，保护密码不受威胁。没有什么方法是完美的。要做出最佳决定，需要理解交互、取舍以及威胁。换句话说，仅遵循一个检查表的规定是不够的，你还需要理解为什么要做检查表所列的事情。

做正确的事情

在拨号访问时期，硅谷有一家公司担心自己的安全。他们担心“战争拨号”，即黑客拨叫一个交换区内所有电话号码，找到一个调制解调器，然后进行密码猜测攻击，因此禁用了调制解调器。

禁用的问题与硅谷流行的习惯产生了冲突，硅谷的研发人员都习惯了衣着随意的在一天的任意时间内工作。研发人员也做了一件事：他们到隔壁商场的计算机专柜，花 29.95 美元买了一个调制解调器接到公司电话线上，然后一整天都开着。公司的安全人员意识到这个问题，于是安装了一个数字电话系统，使得研发人员无法在这个系统中随时使用调制解调器。要使用一个普通的模拟电话线路，需要公司副总经理签字。看起来问题解决了，但是安全人员没有禁止其他的能够连接调制解调器的线路：传真机。因此，一下子很多工程师都提出办公室需要一台传真机，这样的请求被批准了。这些 29.95 美元的调制解调器能够发送和接收传真，当然也并不是 100%的需求造假。

大家都很高兴。安全人员很高兴，因为他们以为没有拨号线路了；工程师很高兴，因为他们能够随意登录。一切都很顺利，直到一个心怀不满的前雇员攻击了这些不安全的防护。而安全人员十分不解，因为他们还以为没有调制解调器呢！

想象一下，如果换一种方式，采用一个集中管理的调制解调器池，通过恰当的认证和登录列表连接到部门人员数据库。这种方式会更加安全，并且会提高生产力，而不是驱使员工去破坏规则。

安全：不需要太多，不需要太少，刚刚好

这两个情形有很多共同之处。更重要的是，它们都说明了安全决策无法凭空产生。这里面有很大一部分人的因素，不与人的行为相匹配的安全解决方案，不管好方案还是坏方案，都会失败。

另外一个相似点是，这些防御通常与实际威胁之间没有匹配好。强密码无法防护按键记录器；此外，无数的用户都认为遵循强密码规则太麻烦。更糟糕的是，他们必须遵守很多套规则，每一套都略有不同。强密码更容易忘记，因此必须依赖密码恢复机制。这些机制通常比原有的认证机制更不安全，Sarah Palin 在电子邮件账号被黑客攻击之后得出了这个结论[Zetter 2010]。她使用的网站花费了很多努力来设计恢复方法、收集和存储数据，以及提出相关问题。从很大程度上讲，他们不得不这么做；人会忘记密码，但是问题是不是首先出现在对强密码的依赖上呢？

禁用调制解调器是为了防止那些恶意拨号的人。他们忽略了内部的威胁，同时也牺牲了一些生产力。他们同样受到其他问题的困扰，例如在零售商那里购买了太多的调制解调器，并且为额外的电话线花费太多。

可能在未来的几年，你的老板将会读到新的 Herkawat 攻击的信息，以及 Kushghab.com 的软件如何来阻止这些攻击。你要买他们的产品吗？如何做出选择呢？我希望你能通过阅读本书，得到这些问题的答案，不仅仅是针对那些随机密码生成器造成的攻击和相关产品是否购买的答案。[①]

对迷惘的一些引导

这本书并非一本安全类的介绍书籍。本书面向的读者对象是系统管理员、IT 管理员、首席安全官以及系统架构师。阅读本书，读者要熟悉防火墙，了解对称加密与非对称加密之间的区别。你可能见过常用的安全检查表，可能获得了某个安全证书，并且拥有证书中描述的能力。我不会告诉你如何避免缓存溢出、跨站脚本攻击，以及 SQL 攻击等，因为已经有很多关于这些内容的书籍了。本书的目的是教会你如何考虑安全决策的内涵，以及如何设计一个架构，来处理安全问题造成的后果。我不知道十年后，网络会变成什么样子，会出现哪些流行的服务和设备。我很确定会有很多新东西出现，一些现在我们想都想不到的东西。你如何保护自己，保护这些新东西，以及保护自己不受新东西的威胁呢？安全检查表是对于知道正确答案的人来说的，但是有时候，正确答案尚未出现。

---

① “APG (Automated Password Generator)”, http://www.adel.nursat.kz/apg/。

本书的第 1 部分是关于理论的。讨论了如何进行思考，同时包含了一些对于可能的威胁的讨论。

第 2 部分讨论一些基本的技术，不仅包括安全技术，例如防火墙，而且包括其他针对无线通信独有特征的技术。

第 3 部分讨论如何创建并且运行实时系统。我们生活在一个不完美的世界，我们需要现在就解决这些问题。

第 4 部分通过对一些案例的学习来掌握这些原则，并且提出对这个领域未来的一些想法。

链接失效说明

George R.R. Martin 写过[G. R. R. Martin 2000]“凡人皆需伺奉，凡人皆有一死”。同样的，网页链接也会失效。我在 2015 年 8 月检查了这本书中的所有 URL，但是当你看到这本书的时候，可能有些链接已经失效了。即使美国最高法院也受这个问题的困扰[Zittrain, Albert, and Lessig2014]。目前，没有什么好办法，试着使用时光机器（https://www.archive.org）可能是最好的选择。

致谢

计算机安全科学不是我创建的，我也不是自学的。我要感谢三位学术泰斗，从他们身上我学到了很多：贝尔实验室的 Fred Grampp、NSA 国家计算机安全中心的 Bob Morris，以及北卡罗莱纳大学教堂山分校的 Fred Brooks。从 Grampp 那里我学到了密码、日志文件以及社会工程学，这很重要。Morris 教会我在展示安全操作系统设计时，考虑其功能，“你如何进行备份和恢复？”他的系统是安全的吗？Morris 还告诉我在评估安全时，经济所处的角色。Brooks 教会我如何考虑软件系统，并让我意识到松散的编码是多么令人痛苦的问题。

我还要感谢在写本书时给过我帮助的所有人。按字母顺序，这些人包括（不仅仅是这些人）：Randy Bush、Bill Cheswick、Richard Clayton、Greg Conti、Simson Garfinkel、Levi

Gundert、Paul Hoffman、Russ Housley、Maritza Johnson、Brian Kernighan、Angelos Keromytis、Brian Krebs、Bala Krishnamurthy、Susan Landau、Fabian Monrose、Kathleen Moriarty、Kevin Poulsen、Avi Rubin、Adam Shostack、Sal Stolfo、Rob Thomas、Win Treese、Paul van Oorschot。还有所有的跟我一起完成这本书的 Addison-Wesley 出版社的人：John Fuller、Stephanie Geels、Julie Nahil、Melissa Panagos、Mark Taub、John Wait 等。当然，本书中出现的错误是我个人的问题。

Steven M. Bellovin
https://www.cs.columbia.edu/_smb

版本信息

这本书是作者使用 LaTeX 撰写的，一些程序包来自于 Comprehensive Tex Archive Network（CTAX），另外还采用了一些自定义宏和环境。

资源下载与勘误

轻松注册成为博文视点社区用户（www.broadview.com.cn），您即可享受以下服务。

- **提交勘误**：您对书中内容的修改意见可在【提交勘误】处提交，若被采纳，将获赠博文视点社区积分（在您购买电子书时，积分可用来抵扣相应金额）。
- **与我们交流**：在页面下方【读者评论】处留下您的疑问或观点，与我们和其他读者一同学习交流。

页面入口：http://www.broadview.com.cn/31066

二维码：

此为试读，需要完整PDF请访问：www.ertongbook.com

目录

第 1 部分　问题定义

第 2 部分　技术

第 3 部分　安全操作

第 4 部分 关于未来

第 1 部分　问题定义

- 第 1 章　介绍
- 第 2 章　对安全的思考
- 第 3 章　威胁模型

此为试读，需要完整PDF请访问：www.ertongbook.com