HZ BOOKS 华章IT
Mc Graw Hill Education

· 网络空间安全技术丛书 ·

HACKING EXPOSED INDUSTRIAL CONTROL SYSTEMS

ICS and SCADA Security Secrets & Solutions

黑客大曝光

工业控制系统安全

[美] 克林特 E. 博顿金 (Clint E.Bodungen) 布莱恩 L. 辛格 (Bryan L.Singer) 亚伦 · 施比卜 (Aaron Shbeeb) 凯尔 · 威尔霍伊特 (Kyle Wilhoit) 斯蒂芬 · 希尔特 (Stephen Hilt) 著 戴超 张鹿 译

武装自己，保护你的 ICS 与 SCADA 系统

机械工业出版社
China Machine Press

黑客大曝光

工业控制系统安全

HACKING EXPOSED INDUSTRIAL CONTROL SYSTEMS

ICS and SCADA Security Secrets & Solutions

[美] 克林特 E. 博顿金 布莱恩 L. 辛格 亚伦 · 施比卜 凯尔 · 威尔霍伊特 斯蒂芬 · 希尔特 著 戴超 张鹿 王圆 译
(Clint E.Bodungen) (Bryan L.Singer) (Sean Bodmer) (Kyle Wilhoit) (Stephen Hilt)

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

黑客大曝光：工业控制系统安全 /（美）克林特 E. 博顿金（Clint E. Bodungen）等著；戴超，张鹿译 . —北京：机械工业出版社，2017.8
（网络空间安全技术丛书）
书名原文：Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions

ISBN 978-7-111-57594-8

I. 黑… II. ① 克… ② 戴… ③ 张… III. 工业控制系统－计算机网络－网络安全 IV. ① TP273 ② TP393.08

中国版本图书馆 CIP 数据核字（2017）第 188610 号

本书版权登记号：图字 01-2017-0721

Clint Bodungen, Bryan L. Singer, Aaron Shbeeb, Kyle Wilhoit, Stephen Hilt : Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions（978-1-25-958971-3）.

Copyright © 2017 by McGraw-Hill Education.

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including without limitation photocopying, recording, taping, or any database, information or retrieval system, without the prior written permission of the publisher.

This authorized Chinese translation edition is jointly published by McGraw-Hill Education and China Machine Press. This edition is authorized for sale in the People's Republic of China only, excluding Hong Kong, Macao SAR and Taiwan.

Copyright © 2017 by McGraw-Hill Education and China Machine Press.

版权所有。未经出版人事先书面许可，对本出版物的任何部分不得以任何方式或途径复制或传播，包括但不限于复印、录制、录音，或通过任何数据库、信息或可检索的系统。

本授权中文简体字翻译版由麦格劳－希尔（亚洲）教育出版公司和机械工业出版社合作出版。此版本经授权仅限在中华人民共和国境内（不包括香港、澳门特别行政区及台湾地区）销售。

版权 © 2017 由麦格劳－希尔（亚洲）教育出版公司与机械工业出版社所有。

本书封面贴有 McGraw-Hill Education 公司防伪标签，无标签者不得销售。

黑客大曝光：工业控制系统安全

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：陈佳媛　张锡鹏　　责任校对：李秋荣

印　刷：北京文昌阁彩色印刷有限责任公司　　版　次：2017 年 10 月第 1 版第 1 次印刷

开　本：186mm × 240mm　1/16　　印　张：21

书　号：ISBN 978-7-111-57594-8　　定　价：89.00 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

版权所有 · 侵权必究

封底无防伪标均为盗版

本书法律顾问：北京大成律师事务所　韩光 / 邹晓东

The Translator's Words 译 者 序

2016 年 2 月，一部名为《 Zero Day 》的纪录片在柏林国际电影节上映，这部影片在烂番茄影评网站上获得了平均为 7.4 的评分（同年《美国队长 3：英雄内战》平均评分为 7.6），影片纪录了一起在 2010 年人们广泛关注的恶意代码攻击事件：一款名为 Stuxnet 的蠕虫发起了针对西门子公司数据采集与监控系统 SIMATIC WinCC 的攻击。自此，针对工控系统的潘多拉魔盒被打开了……

Stuxnet 蠕虫攻击事件发生之后，人们纷纷将目光聚焦到了工业控制系统之上。那么，工业控制系统是什么？与物联网、工业 4.0、工业物联网、SCADA 相比，工控系统有什么区别？针对工控系统的攻击为什么会造成那么大的破坏？我们如何来保障工控系统的安全？等一系列问题纷至沓来。

根据美国国家标准技术研究院（NIST）给出的定义，工业控制系统（Industrial Control System，ICS）是多种控制系统的总称，包括监控和数据采集系统（SCADA）、集散控制系统（DCS），以及工业部门和关键基础设施中常见的可编程序控制器（PLC）等控制系统。工业控制系统通常由共同作用以期实现某一工业用途（例如，物质或能量的制造、运输）的控制部件（例如电器、机械、液压、气动）组合而成。当前，工控系统已经广泛应用于电力、石油、天然气、核能、化工、食品、医疗、水利、交通等众多关键基础设施之中。

早期的工业控制系统同互联网物理隔离，且大多采用专用软硬件，因此即便工控系统中存在安全隐患，但外界既难以接触到工控系统也难以展开对工控系统的研究。但是，随着 IT 技术在工业环境中的广泛应用，通用计算设备、通用操作系统开始用于工控系统的实现，工控协议也开始基于 TCP/IP 协议构建，传统 IT 系统所面临的威胁蔓延到了工控系统环境当中。尤其自从 2010 年 Stuxnet 蠕虫出现以来，针对工控系统领域的关注度飙升，2011 年至 2015 年工控系统的安全事件经历了一段时期的快速增长，直到 2016 年增速才逐

渐放缓。[⊖]

虽然同传统 IT 技术之间存在着千丝万缕的联系，然而由于工业控制系统在结构和作用上的特点，使得其同传统 IT 系统安全相比呈现出了诸多区别：

❑ 工控系统设计时未从信息安全角度进行考量

工控系统在设计时大多仅仅考虑了功能安全，即确保工控系统能够正确执行其功能，并且当系统失效或出现故障时，设备或系统仍然能够处于安装状态或进入到安全状态。但是，工控系统环境中的设备、协议及应用程序在设计之初并没有考虑到信息安全问题。某些情况对于 IT 网络而言通常是正常的，然而在工控系统环境中却可能带来不可逆转的负面影响。而且，工控系统中的应用程序和协议最初都是在没有考虑认证和加密机制以及常见网络攻击方式的情况下设计开发的。

❑ 工控系统中信息安全三要素的优先级不同

传统 IT 系统安全中的三要素分别是保密性、完整性和可用性，但是在工控系统中需要对三要素的顺序进行调整。对于工控系统而言，系统的可用性至关重要，因此需要将可用性放在考虑安全问题的第一位，即可用性、完整性、保密性。此外，优先级的变化不仅仅体现在安全要素的排序之上，更关键的是在应对工控系统安全问题时按照该优先顺序考虑问题。

❑ 工控系统设备的处理能力过载阈值较低

许多工控系统设备，比如 PLC 与 RTU 均用到了嵌入式处理器，而嵌入式处理器在特定条件下可能非常容易过载。当嵌入式处理器过载时，就可能会对设备的可用性造成影响，导致包括设备响应中断、复位、故障、网络通信中断，甚至出现配置丢失的情况。

❑ 工控系统设备的网络堆栈处理能力较弱

很多工控系统设备处理异常流量的能力较为薄弱。当向工控系统设备发送异常流量时，例如超长数据包、畸形数据包、高速网络包，抑或是未使用预定协议的数据包，也会导致设备响应中断、复位、故障、网络通信中断等情况。

❑ 工控系统环境中大量使用遗留的老式系统

无论是控制设备本身还是老式的服务器与工作站，大多数工控系统环境中依然保留有大量遗留的老式系统，这些老式系统甚至还在使用 Windows XP、Windows NT、Windows 95 等操作系统。这些遗留的老式系统不仅有些已经停止更新，而且即便是安装某些软件对其进行加固都可能会导致资源耗尽与系统崩溃。

❑ 工控系统网络的网络带宽较低

⊖ 数据来源：ICS-CERT《Year in Review 2016》(https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2016_Final_S508C.pdf)，FireEye《OVERLOAD，CRITICAL LESSONS FROM 15 YEARS OF ICS VULNERABILITIES——2016 Industrial Control Systems (ICS) Vulnerability Trend Report》(https://www.fireeye.com/blog/threat-research/2016/08/overload-critical-lessons-from-15-years-of-ics-vulnerabilities.html)

试读结束：需要全本请在线购买： www.ertongbook.com

同传统的业务 IT 网络相比，许多工控系统网络用于网络连接的网络带宽较低，其原因在于工控系统使用了老旧的网络设备或者使用了工业无线网络，其中也包括移动宽带和卫星通信。所以，引入高速网络流量可能会导致网络延迟甚至网络通信的中断，哪怕看似无害的网络流量也可能会导致部分工控系统网络的延迟。而对于高可用性网络，延迟也是不可接受的。

❑ 工控系统补丁更新不及时且难以应用

大多数工控系统环境都无法像传统的 IT 系统环境那样经常定期发布补丁。而且，对于基于老式操作系统开发的工业控制系统，甚至可能已经没有厂家能够提供可用的安全补丁。同时，由于工控系统软件与其底层之间紧密耦合，补丁更新必须进行代价高昂、耗时甚多的回归测试。而对补丁更新后的软件进行测试以及补丁后续分发过程中的耗时，则可能导致工控系统在一段相当长的时间范围内存在漏洞。此外，工控系统本身所具有的关键性和敏感性也使得对其进行补丁修复工作较为困难，工控系统中的很大一部分属于“高可用性”系统，因此在定期维护时间窗口之外进行关机来安装更新和补丁程序通常是不现实的。即使是在定期维护时间窗口之内，许多传统的网络安全措施（如反病毒软件、安全更新和补丁）也都有可能对工控系统设备和网络产生负面影响。

基于工业控制系统的自身特点，本书从渗透测试的角度介绍了针对工控系统进行安全研究所涉及的诸多方面，必将为工控系统的研究人员提供有益的参考。全书的组织结构与概要如下：

全书共分三个部分：

第一部分包括第 1 章至第 3 章，主要对工控系统的架构与组成、工控系统的风险评估以及工控系统的威胁情报进行介绍。

这一部分主要回答了以下问题：

❑ 工控系统主要功能有哪些？

❑ 工控系统中的普渡参考模型是什么？

❑ 常见的控制系统有哪些？

❑ 工控系统风险评估的评估与度量对象有哪些？

❑ 如何针对工控系统开展风险评估？

❑ 工控系统威胁情报的概念与作用是什么？

❑ 工控系统环境中如何开展威胁建模？

第二部分由第 4 章至第 8 章组成，主要对工控系统渗透测试、协议、设备、应用以及针对工控系统的“0-day”漏洞挖掘与恶意代码进行介绍。

这一部分主要回答了以下问题：

❑ 工控系统渗透测试的测试方法有哪些？

❑ 针对工控系统与 IT 系统开展渗透测试的区别有哪些？

❑ 如何部署工控系统渗透测试环境？

- ❑ 工控系统渗透测试的测试策略都有哪些？
- ❑ 工控系统主要采用哪些协议？针对这些协议主要有哪些攻击方式？
- ❑ 针对工控系统设备与应用主要有哪些攻击方式？
- ❑ 如何着手开展工控系统“0-day”漏洞研究？
- ❑ 针对工控系统的恶意代码有哪些类型？各有什么特点？

第三部分包括第 9 章和第 10 章，对工控系统安全标准及风险缓解策略进行介绍。

这一部分主要回答了以下问题：

- ❑ 工控系统合规性与安全性之间有什么关系？
- ❑ 常见的工控系统安全标准有哪些？
- ❑ 从哪些角度考量有助于缓解工控系统常见风险？如何缓解？
- ❑ 工控系统的风险缓解过程包含哪些步骤？

本书第 3 章至第 8 章由戴超翻译，第 1 章、第 2 章、第 9 章、第 10 章由张鹿翻译，全书由戴超、张鹿进行审校。在前期翻译过程中，王圆博士也开展了大量工作，在后期审校过程中，海康威视网络与信息安全实验室王滨博士、北京理工大学王安博士提供了大量宝贵意见，在此一并表示衷心的感谢。最后，感谢华章公司的编辑朱劼、张锡鹏、陈佳媛在本书翻译过程中提供的帮助，感谢他们的全力支持与耐心指导，在全书的翻译过程中使我们少走了很多弯路。

在阅读本书的过程中，读者可将错漏之处与问题反馈给我们，联系邮箱为 icsquestion@163.com，希望广大读者不吝赐教。

戴超　张鹿

2017 年 3 月

About the Authors 作者简介

Clint Bodungen（休斯顿，得克萨斯州）

Clint Bodungen 是卡巴斯基实验室的一名关键基础设施安全高级研究员。在“网络”（cyber）安全行业拥有二十余年的从业经历，专门从事风险评估、渗透测试以及脆弱性研究。Clint Bodungent 过半的工作经历都关注于工业控制系统。Clint Bodungen 从 11 岁起开始编程，并在 20 世纪 90 年代中期为 Unix/Linux 操作系统开发应用程序与工具。在美国空军服役期间，Clint Bodungen 的职业生涯拉开了序幕，他拥有工业设计技术学位并先后担任了单位的计算机系统安全官（Computer Systems Security Officer，CSSO）及 OPSEC 主管。Clint Bodungen 在 Symantec 公司任职并对公司研发的 IDS 应用程序进行测试期间热衷于威胁研究与系统测试。2003 年，一家工业自动化咨询公司聘请 Clint Bodungen 来帮助某家大型石油和天然气公司对其 SCADA（Supervisory Control and Data Acquisition）系统进行安全保障，自那以后 Clint Bodungen 开始对工业控制系统有所涉猎。此后，Clint Bodungen 领导了多项美国顶级能源机构的工业控制系统风险评估和渗透测试项目，并继续同工控系统厂商一起致力于脆弱性研究。Clint Bodungen 设计并教授了十多门工控系统安全培训课程，并多次在工控系统网络安全大会上发表演讲。

Bryan L. Singer，CISSP，CAP（蒙特瓦洛，阿拉巴马州）

Bryan Singer 是 Kenexis 安全公司的主要投资人之一，重点关注工控系统以及 SCADA 系统安全问题，是一名业内公认的工业安全专家。Bryan Singer 曾服役于美国陆军，从一名空降兵成长为情报分析员。此后，Bryan Singer 多次参与大型工业网络架构及网络安全架构的设计、开发与实施工作，并在全球多个关键基础设施领域开展渗透测试与网络安全评估工作，涵盖领域包括电力、石油和天然气、食品饮料、核能、汽车、化工及制药等。Bryan Singer 2002 年开始担任 ISA-99/62443 标准委员会的创始主席，直到 2012 年卸任。Bryan Singer 擅长的技术包括软件开发、逆向工程、电子取证、网络设计、渗透测试以及网络安全脆弱性评估等等。Bryan Singer 现居住于阿拉巴马州的蒙特瓦洛，多次就工控系统安全领域的问题撰写文章、发表演讲并分享经验。

Aaron Shbeeb（休斯顿，得克萨斯州）

Aaron Shbeeb 早在少年时期就对程序开发及计算机安全产生了兴趣。他毕业于俄亥俄州立大学，获得了计算机科学与工程理学学士学位。Aaron Shbeeb 在软件开发以及安全岗位拥有十多年的从业经验，主要关注安全程序设计实践。从 2008 年起，在职业发展以及个人兴趣的双重驱动下，Aaron Shbeeb 开始从事针对工控系统 /SCADA 系统的渗透测试以及安全研究工作。

Stephen Hilt（查塔努加，田纳西州）

Stephen Hilt 在信息安全与工控系统安全领域工作了十余年。从南伊利诺伊大学获得学士学位后，Stephen Hilt 供职于美国一家大型电力公司。在该公司就职期间，Stephen Hilt 在安全网络工程、事件响应、电子取证、评估以及渗透测试领域积累了丰富的经验。随后，Stephen Hilt 开始关注工控系统评估以及 NERC CIP（North American Electric Reliability Council，Critical Infrastructure Protection）评估工作。鉴于其从业经历，世界上最著名的工控系统安全咨询公司 Digital Bond 聘请他担任工控系统安全顾问与研究员。2014 年至 2015 年期间，Stephen Hilt 发布了针对工控系统的众多 Nmap 脚本，通过本地命令对工控系统协议进行识别。目前，Stephen Hilt 担任 Trend Micro 公司的高级威胁研究员，继续从事工控系统研究工作，并在其他高级研究领域开展了深入的探索。

Kyle Wilhoit（费斯图斯，密苏里州）

Kyle Wilhoit 是 Trend Micro 公司的一名高级威胁研究员，主要关注于捕获互联网上的恶意代码。在加入 Trend Micro 公司之前，Kyle Wilhoit 就职于 FireEye 公司，主要关注国家层面的攻击者。只要 Kyle Wilhoit 没有去周游世界，你就可以在他的家乡圣路易斯找到他。

About the Contributor and Technical Editor 技术审校者简介

W. Stuart Baily（休斯顿，得克萨斯州），拥有 CISSP、GICSP 认证，是一名在企业与工业控制系统网络领域拥有 17 年从业经验的 IT 安全专家。Stuart 在医疗领域开始他的职业生涯，先后任职于一家大型临床系统和得克萨斯医疗中心的 Baylor 医学院，其间经历了网络、服务器以及安全等团队中的多个岗位。Stuart 随后就职于 Noble 能源公司的上游石油与天然气部门，他在该部门制订了控制系统的安全方案，并激发出了对于工控系统安全的热情。现在，Stuart 在得克萨斯州一家公共事业机构的安全团队工作。在开展陆海油气勘探和生产设施的现场安全评估、设计控制系统事故响应计划、拟制工控系统安全策略与程序、开展安全意识培训、提供新立工控系统项目咨询和评估部署新型工控系统软硬件等方面，Stuart 积累了丰富的经验。

前　言 *Preface*

黑客大曝光——工业力量

毫无疑问，本书沿袭了《黑客大曝光》系列书籍的一贯风格。无论称之为渗透测试（penetration testing 或 pentesting）、道德入侵（ethical hacking）还是红队测试（red team testing），本书主要从攻击的角度研究网络安全问题。而且，在本书中，我们主要研究工业控制系统（Industrial Control Systems，ICS）的网络安全（不管读者喜不喜欢，主题已经剧透出来了），根据情况也可以称之为 *in*-security。

监控和数据采集系统（Supervisory Control and Data Acquisition，SCADA）、**工业控制系统**（ICS）以及**运营技术**（Operations Technology，OT）都是最近在提到工业系统时常用的“万能”术语。如果真想深究营销术语，还可以将**工业物联网**（Industrial Internet of Things，IIoT）添加进去。不过，先将这些热门词汇抛在一边，除了很多其他的行业术语，例如：过程控制域（Process Control Domain，PCD）、过程控制网络（Process Control Network，PCN）、过程控制系统（Process Control System，PCS）、集散控制系统（Distributed Control System，DCS）等，还有监控和数据采集系统（SCADA）以及工业控制系统（ICS）也都旨在描述工业系统特定但又互不相同的方面。但是，这两个术语经常被错误地互换使用。有鉴于此，为了简单起见，本书中我们使用“工控系统”（ICS）来指代工业系统的所有方面，即便我们知道这个术语未必在每种场合下都是正确的。

渗透测试……确定要在工业控制系统中进行吗

从传统角度来讲，当从“红队”或者说从攻击角度来讨论工控系统网络安全时，通常会遭到持怀疑态度并且忧心忡忡的工业资产所有者和运营人员的强烈排斥。从“蓝队”或者说从单纯的防御角度已经出版了若干本内容翔实的工控系统安全图书，然而在我遇到的

试读结束：需要全本请在线购买：　www.ertongbook.com

来自不同工业部门的人员中，还是有人认为那些详细介绍“工控系统入侵”（ICS hacking）技术的图书压根儿就不该出版。这一“理论依据”主要是源自于这样一支思想流派：他们认为类似的信息（甚至包括向部分人士披露有关工控系统的漏洞）都应该妥善保管起来，只有特定的专业团队还有信息共享和分析中心（Information Sharing and Analysis Centers，ISAC）才能够获取这些信息。这一方法也被看作是一种阻止黑客获取敏感信息的努力。因为很多人担心这类信息会帮助黑客们制订工控系统攻击方案或者“入侵攻略”。而细究起来，这种“策略”其实是“不公开即安全”（security through obscurity）的另一种形式，IT 社区早在 20 年前也是这样的心态。这也正是整个行业中工控系统安全的领军人物经常说“工控系统的安全落后于其他行业十多年”的原因之一。

但是，真相是黑客们已经知道了这些信息，或者最起码知道如何获取这类信息，不论业界已经尽了多大努力来隐藏它们。不管用户喜不喜欢，通过主流的隔离措施与不公开的方法已经难以实现对工业系统的保护。正所谓木已成舟，已成定局。既然攻击者已经知道了工控系统和 SCADA 系统的存在，并且了解了它们的重要性，而且坦率地讲，攻击者也清楚它们到底有多脆弱，那么自然会对开展攻击燃起狂热的兴趣。事实上，与资产所有者以及运营人员在学习入侵技术以及如何实施入侵方面所付出的时间相比，黑客们往往花费了更多时间来学习工控系统，以及如何入侵这些系统。支撑这一发现的证据可以从世界各地众多“黑客”大会的会议日程中清晰地看到，例如著名的 Black Hat 和 DefCon，而这只是其中的两个会议。事实上，大多数安全会议现在都会开辟出特色鲜明的“工控系统小镇”，让与会者可以体验一把工控系统设备的入侵。无论读者是否相信，工控系统入侵正在迅速成为主流话题。实际情况是，限制该类信息的获取不仅难以阻止黑客们获取信息，反而阻碍了真正需要这类信息的人们获取信息（工业资产所有者以及运营人员），更不要说工业社区中已经共享了大量关于安全事件和漏洞的信息。然而，关于工控系统漏洞利用以及入侵技术的重要信息往往会被忽视。

为什么了解攻击技术这么重要？简言之就是，如果能够像攻击者一样思考，并且了解其做法，那么就有更多的机会阻挡攻击者的入侵。想想看，以读者最喜欢的运动为例（无论是团队的还是个人的），是否有人在不了解对手攻击方式的情况下就踏上赛场？当然了，肯定会有这种情况，但是在这种情况下，通常是场有利于对手的一边倒的比赛。在对对手的攻击策略与攻击方法一无所知的情况下，实施针对攻击的有效防御是相当困难的一件事。在工控系统网络安全领域中也是这样。对攻击、漏洞利用和恶意代码感染的方法与技术细节越了解，有的放矢地开展防御就越准确、越高效，性价比也越高。考虑一下，下面哪种方法听起来更加高效、性价比更高？

1）以“层次防御”以及网络安全标准合规性的名义，尽可能多地尝试采用一揽子“最佳实践”。

2）对于经过验证得出的的确存在漏洞的地方，根据其潜在影响的严重程度进行优先级排序，针对最有可能面临的威胁部署相应的对抗措施。

如果回答是“1”，那么恭喜啦，因为你肯定拥有巨额的网络安全预算还有大量合格的工作人员！但是即便如此，仍然需要针对试探性的攻击威胁构建安全保障网。

对于存在合规要求的某一行业来说，合规性通常是其实施和改进网络安全控制措施的唯一强制驱动力，其预算往往捉襟见肘，即便如此，聘请渗透测试人员仍会体现出巨大的价值。事实上，预算不足正是渗透测试的用武之地。在结合适当的风险评估过程（详见第 2 章）使用时，渗透测试（详见第 4 章）与威胁建模（详见第 3 章）相结合的方式能够提供更有针对性而且更加高效的风险管理策略。由于具备同恶意攻击者一样的技术水平和知识储备，渗透测试人员能够帮助验证潜在威胁是否确实会对系统构成巨大风险（同只采用传统的风险评估方式相比具有更高的准确性）。这些信息有助于改进风险缓解策略、明晰目标资源中需要关注的重点、确定可以“接受”哪些风险，从而降低对目标资源（金钱、时间和人力）的影响。

很多人不会立即将渗透测试和威胁建模关联起来。但是，渗透测试人员在网络攻击方法方面所具备的经验与知识储备在威胁建模过程中确实是非常宝贵的资源。

当谈到工控系统的可用性、正常运行时间以及功能安全时，（由于渗透测试通常具有主动性和侵入性的特点）往往会存在一些对渗透测试的偏见。如果未经规范培训的测试人员没有采用能够保障工控系统安全（“ICS safe”）的测试方法，这种担心确实不是空穴来风。很多在 IT 系统中没有危害的渗透测试方法可能会在工控系统环境中出现副作用，以至于给安全与生产带来风险。甚至非常简单的测试方法，比如端口扫描在工控系统环境中通常也是禁止的。

所以，如何应用渗透测试来保障工控系统安全呢？首先，本书将教会读者在不影响生产系统的前提下，如何应用针对工控系统的渗透测试方法与技术。其次，我们意图展示如何通过以基于威胁建模的方法应用渗透测试知识，甚至在无须开展主动渗透测试的情况下，制订出更加高效（以及性价比更高）的风险缓解策略与部署方案。

本书所涵盖的内容

无论是作为工控系统渗透测试指南还是用于离线威胁建模，本书旨在帮助读者了解攻击者所具备的“攻击性”知识，使读者在风险管理方面所做出的努力具有更高的准确性与性价比。我们在这里使用术语“管理”的原因在于风险缓解并不总是最优的选择。在某些情况下，最优的解决方案可能只是降低、接受或者转移风险。

依据若干工业安全标准所提出的要求，必须开展渗透测试，而且渗透测试也应该成为每个风险管理项目的一部分，但我们的本意并不是为具体的工控系统网络安全标准提供“合规性”指南。本书也无意于作为工控系统风险缓解或管理技术的专用指南。正如前文提到的，从这一角度出发已经出版了很多书籍，因此没有必要再进行重复。而我们将要分析研究的风险缓解技术以及对抗措施则与本书中介绍的攻击方式与策略密切相关。

我们将会讨论在 CVE 以及 ICS-CERT 公告中已经公开披露的几个漏洞及其众多技术细节，还有相关的漏洞利用技术。但是，在工控系统厂商以及其他业界成员开始提心吊胆之前，需要指出的是我们不会披露 0-day 漏洞（未公开漏洞）与漏洞利用工具。本书中所讨论的全部内容都可以采用各种方式公开查询得到。我们所做的仅是对其中部分 CVE 与 ICS-CERT 公告进行剖析和研究，以展示如何开展针对工控系统设备、应用程序与环境的渗透测试、脆弱性研究以及威胁建模。

本书也不打算对工控系统或者通用渗透测试方法进行全面介绍。但是，当我们认为出于功能所需并且与上下文相关时，将会提供辅助资料，或者在需要进一步指导或者额外信息的事件中指明正确的方向。例如，部分读者可能并不了解工控系统环境的运行机制，所以本书将从较高的层面对工控系统进行有一定深度的基础介绍，以帮助读者理解本书的内容。（那些对工控系统已经有深入了解的读者可以忽略这部分内容。）类似地，还有部分读者可能对渗透测试的基础内容不太熟悉，对此本书也提供了大量关于传统渗透测试方法的参考资源，涵盖了从基础入门到高级技巧的所有内容。

我们的总体目标主要关注于本书各主题所涉及的同工控系统有关的细节。放心好了，对于想要进一步获取本书未涉及的细节以及指导的读者，我们也提供了资料、链接，以及参考文献以供读者进行更深入的了解。

本书面向的读者

本书可以作为对工控系统网络安全感兴趣的读者的参考用书，但是，最终本书面向的对象是对工控系统有关的脆弱点、威胁或威胁建模，以及渗透测试技术等技术细节感兴趣的读者，包括：

- 承担针对工控系统的渗透测试项目，以及希望了解工控系统渗透测试技术的渗透测试人员
- 监控工控系统网络的网络安全分析人员
- 工控系统网络安全威胁情报分析人员
- 致力于工控系统相关设备与应用程序漏洞挖掘的研究人员
- 研发适用于工控系统设备、应用、网络产品的网络安全产品开发商
- 工控系统厂商
- 对工控系统渗透测试技术感兴趣的网络安全爱好者以及渗透测试人员

其他对本书感兴趣的读者群体包括：

- 工控系统资产所有者以及负责招聘渗透测试团队的管理人员
- 工控系统资产所有者以及负责工控系统安全团队的管理人员

虽然这些读者群不需要知道工控系统渗透测试过程中的所有技术细节，但是他们应该对工控系统网络安全威胁与渗透测试技术有一个大概的了解。

本书的组织方式

在学习本书的过程中无须逐页阅读。例如，对工控系统环境已经非常熟悉的读者可以跳过第 1 章。渗透测试人员则可以直接跳到与其当前测试内容有关的具体章节。不过，书中每个主题的安排顺序均同现实中渗透测试项目的实施流程相一致。所以，为了了解工控系统渗透测试的全过程，从头开始逐页阅读也是个不错的选择。资产所有者以及管理人员也可以采用这种方式，来获取对整个工控系统渗透测试和威胁建模过程，以及各组成部分的完整认识。

本书的每一部分都会安排案例分析。这些案例分析虽然是虚构的，但是其背后蕴含的内容都是由可行的事件所组成的，将这些内容组合起来可以构成一个完整的场景。故事中涉及的特定行业、系统以及装置设备的细节并未明确描述，所以来自不同行业的读者都可以从中找到与自己行业似曾相识的感觉。在阅读这些案例分析时，读者可以尝试着将自己带入工控系统安全专家的角色，看看自己能否找出故事中的机构、人员所犯下的错误，正是这些错误最终导致了信息泄露以及入侵攻击。关于这些案例分析中用到的方法、技术的参考文献和技术细节可以在每个案例分析的结尾位置或者案例分析所在的章节中找到。对抗措施在全书都可以找到，也可以在第三部分找到。

第一部分（第 1 章至第 3 章）主要包括从较高层面构建渗透测试项目的相关内容，为后续内容做铺垫，并对工控系统、风险评估以及威胁建模过程进行了简短概述。

第二部分（第 4 章至第 8 章）深入介绍了工控系统渗透测试过程中的细节。首先对工控系统渗透测试策略进行了概述，然后以《黑客大曝光》式的风格介绍了细节、技术以及实例。为了更详尽地涵盖工控系统渗透测试技术的方方面面，我们对工控系统设备、应用程序以及协议中最常见漏洞类别中的部分样本进行了分析。每类都表示若干种相关的、现实中已经披露的漏洞，包括与之关联的 ICS-CERT 公告。本着渗透测试的“完整性”原则，本书就工控系统漏洞研究进行了高级进阶内容的入门介绍（再提醒一下，书中未披露现实中存在的任何 0-day 漏洞）。由于恶意代码迅速成为工控系统安全中的一个重要主题，所以我们对工控系统恶意代码也进行了分析，并介绍了其实现机制及对抗措施。

第三部分（第 9 章和第 10 章）主要通过研究工控系统网络安全策略来形成风险评估过程的闭环，但是仅仅涉及了本书中讨论到的攻击技术。正如前文所述，已有大量内容对工控系统网络安全对抗措施进行介绍，我们会在适当的位置做出提示帮助读者获取相关信息。本部分的目标是帮助读者针对攻击采取正确的响应与对抗措施。因此，为了便于参考，针对各自章节攻击方式所提出的对抗措施也均会进行相应的总结。

最后，第四部分的附录中包含了术语表以及在风险评估、威胁建模及渗透测试项目中卓有成效的流程图和图表。

各章概述

下面是对各个章节的概要，分别对各章节的内容进行了简要介绍。

第一部分　做好准备：工业控制系统渗透测试就位

第 1 章　工业控制系统安全概述

从较高的层次简短介绍工控系统架构、组成部分、功能以及术语等方面，读者能够获取到理解本书概念所需的基本工控系统知识。

第 2 章　工业控制系统风险评估

就如何在工控系统风险评估过程应用本书内容以及如何根据环境开展工控系统渗透测试提供了一个简短的高级指南。

第 3 章　通过威胁建模获取具有可操作性的工业控制系统威胁情报

虽然数十年来术语威胁情报（threat intelligence）在情报界一直是个不可或缺的概念，但是在工业界中则是最近才流行起来的一个时髦词汇。本章讨论了如何利用威胁情报以及如何利用获取的相关资源对工控系统风险管理策略进行改进。

第二部分　工业控制系统入侵

第 4 章　渗透测试策略

为了得到准确、符合实际的结果以及保护运营过程的功能安全，必须拟定合适的工控系统策略。本章主要基于现实的风险场景讨论工控系统渗透测试策略，并就避免对工控系统生产环境造成影响的方法与步骤进行了概述。

第 5 章　工业控制系统协议攻击

本章详细介绍了在常见工控系统协议中发现的漏洞以及与之对应的漏洞利用技术。

第 6 章　工业控制系统设备与应用攻击

本章结合 ICS-CERT 公告，研究了工控系统设备和应用程序的漏洞，以及相应的漏洞利用技术。

第 7 章　工业控制系统“0-day”漏洞研究

大部分渗透测试依赖于众多的已知漏洞。但是，未披露甚至未发现的漏洞（即 0-day 漏洞）却会带来更加严重的问题。因此，具备独立挖掘未公开漏洞的能力在风险管理策略中会赋予策略制订者以关键优势。虽然仅仅一个章节不足以涵盖漏洞研究的方方面面，但是，本章不仅对工控系统漏洞挖掘策略进行了概述，还提供了可供进一步研究的关键资源。

第 8 章　工业控制系统恶意代码

自从 2010 年遭受 Stuxnet 攻击以来，工业界清醒地认识到恶意代码已经将工控系统环境作为了攻击目标，并且确实能够对工控系统环境造成影响。自从那时起，众多攻击活动均以 Stuxnet 为模板，开发出了针对工控系统的恶意代码，用以潜入、感染关键系统，甚至对关键系统造成破坏。本章分析了恶意代码开发人员在编写专门针对工控系统环境的恶意代码时所用到的结构、机制及技术。最后，为了帮助读者对恶意代码所能造成的工控系统威胁拥有更加深入的认识，本章对部分现实中针对工控系统的知名恶意代码攻击活动进行了介绍。

第三部分　融会贯通：风险缓解

第 9 章　工业控制系统安全标准入门

本章对常见的工控系统网络安全标准，以及这些标准同本书中所提及的技术与内容的

关联进行了简要介绍。

第 10 章　工业控制系统风险缓解策略

虽然本书并不想成为一本关于工控系统网络安全对抗措施技术的详细指南，但第 10 章仍然对与本书主题相关的工控系统风险缓解策略及对抗措施进行了介绍。

第四部分　附录

附录 A　缩略语表

附录 A 中的内容是工控系统网络安全中常用的缩略语。

附录 B　术语表

附录 B 中的内容定义了工控系统网络安全中常用的术语。

附录 C　工业控制系统风险评估与渗透测试方法流程图

附录 C 中提供了一组开展工控系统风险评估以及渗透测试的模板与流程图。

基本组成模块：攻击与对抗措施

同其他带有《黑客大曝光》题目的图书一样，本书的基本组成模块也是在“入侵”章节中所讨论的攻击与对抗措施。本书中对攻击的强调方式同整个《黑客大曝光》系列中的其他图书一样：


攻击图标

采用这种图标对攻击进行强调可以很容易地识别出特定的渗透测试工具和方法，帮助读者快速定位到说服管理层为新安全计划提供资金支持时所需要的信息。当涉及对抗措施时，我们也遵循了“黑客大曝光”系列图书采用的一贯方式，在每次介绍完一种攻击方式或者一系列相关的攻击方式之后，紧接着介绍对抗措施。对抗措施的图标也保持不变：


对抗措施图标

该图标提醒读者下面介绍的将是关键修复信息。

在第 5 章和第 6 章中对每种攻击方式的风险评级是这样计算的，首先对各攻击方式的流行度、难易度以及影响力进行赋值，然后对各单项得分取平均值。

流行度：	*流行度基于实施攻击的工具的可用性，1 表示可用性最低，10 表示可用性最高*
难易度：	*难易度基于攻击实施的难易程度，例如，如果需要操作某些数据包来开展攻击，那么 1 表示最困难，10 表示最容易*
影响力：	*影响力是如果攻击成功对工控系统的影响程度，1 表示影响最小，10 表示造成了关键影响*
风险评级：	*上述 3 个值的平均值即整体的风险评级*

试读结束：需要全本请在线购买：　www.ertongbook.com