Secrets and Lies:
Digital Security in a Networked World

网络与信息安全技术丛书

网络信息安全的真相

《应用密码学》姐妹篇
Schneier 的又一力作

(美) Bruce Schneier 著
吴世忠 马 芳 译

机械工业出版社
China Machine Press

WILEY

网络与信息安全技术丛书

网络信息安全的真相

（美） Bruce Schneier 著

吴世忠 马芳 译

机械工业出版社
China Machine Press

本书介绍计算机系统的安全性问题、技术的局限性以及解决方案。本书用大量实例，生动地描述了系统中的各种安全环节，并阐述作者独特的见解。本书适合系统设计与分析人员参考，也适合研究安全问题的技术人员和想了解安全问题的普通读者阅读。

本书版权登记号：图字：01-2001-0488

图书在版编目(CIP)数据

网络信息安全的真相/（美）斯克内尔（Schneier, B.）著；吴世忠等译. -北京：机械工业出版社，2001. 9
（网络与信息安全技术丛书）
书名原文：Secrets and Lies: Digital Security in a Networked World
ISBN 7-111-09191-4

Ⅰ.秘.. Ⅱ.①斯...②吴... Ⅲ.计算机网络-安全技术 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2001)第 055726 号

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：周志全 张鸿斌
北京牛山世兴印刷厂印刷 · 新华书店北京发行所发行
2001 年 9 月第1版第1次印刷
787mm × 1092mm 1/16 · 15.75 印张
印数：0 001 - 5000 册
定价：35.00 元

译 者 序

在颇具神秘色彩的密码学和信息安全领域中，Bruce Schneier 先生称得上是一匹黑马。几年前，在全球信息安全炙手可热的时运下，他凭着对应用密码学全景式的盘点和家珍般的评说，以《应用密码学》（中译本由机械工业出版社引进出版）一书横空出世。将密码学在信息安全中的强大生命力阐述的淋漓尽致。就在这本被人誉为“编码黑客的圣经”的密码学专著以多种文字畅销全球的时候，Schneier 又推出了另一部新书，这本新书篇幅不长，但却有一个很长的名字——《秘密与谎言：网络世界中的数字安全》（英文原著的直译名），同时有着十分鲜明的主题：那就是要揭示信息安全的真相。用 Schneier 先生自己的话来说，他写这本书部分是为了纠正一个错误，纠正他在《应用密码学》中将密码学视为灵丹妙药的神话。他坦陈：“密码学是数学的一个分支，它涉及到的是数学、公式和逻辑。我们生活中的安全涉及到的则是人：人所知道的事情，人际之间的关系，人和机器的关系等。而数字安全涉及到的却是计算机：各种复杂的、不稳定的、甚至充满漏洞的计算机。”Schneier 用完全非技术的语言说明密码学与计算机安全的关联和区别，从现实社会和网络生活的角度阐述了自己对信息安全问题的深切理解。

本书共分三大部分。第一部分用四章的篇幅勾勒出数字安全的观念背景。作者对安全威胁的概括不仅包括各种刑事攻击，而且还涉及了名声攻击和法律性攻击，并将攻击者类分为国家情报机关、新闻机构、恐怖分子、内部奸细、犯罪分子和产业间谍等，作者归纳了人们的安全需求：内容包括隐私保护、匿名需要、完整无缺、身份识别和审计跟踪等。

第二部分探讨的是包括密码技术、软件可靠性、安全硬件、识别与鉴别和证书与凭证在内的安全技术和包括计算机、联网计算机和网络安全等在内的安全域。还用一章专门讨论信息安全的“人为因素”。从移动代码的问题、到安全硬件的采用、直至数字证书的局限，Schneier 用简洁明了，非技术性的语言对信息安全的技术及其局限性进行了独到的分析，通过例证纠正了不少人们在安全问题上的常识性错误。

在第三部分中，作者探讨的是安全策略，内容包括安全管理的方方面面。例如脆弱性、攻击方法和对应措施，特别强调了威协建模和风险评估的重要性，作者还讨论了产品的测试和检验，以及产品未来的发展。在本书结尾，作者再次强调了自己对安全真相的理解，那就是：信息安全是基于风险评估的，“安全并非某一个产品，它是一个完整的过程。”

作者恳请每一位读者从头到尾通读本书，一方面是因为该书确实象一个故事，情节跌宕，前后呼应；另一方面是因为该书将复杂的信息安全技术用非技术性的语言娓娓道来，专业人士也好，非专业人员也罢，均能看得明白。综观这本一气呵成的著作，精彩章节着实不少，比如在讨论密码学的第 6、7 章中，作者对加密概念及内容的高度概括和对专用算法存在问题的精辟分析着实令人叫绝。在“识别与验证”一章中对口令字存在的问题和生物统计学方法

现有局限的分析也是入木三分。在“软件可靠性”一章中对堆栈溢出的精彩描述更是难以在别处见到，而读了“产品的测试与检验”一章，你不得不承认，除了密码学而外，评价软件的安全缺陷应是 Schneier 的另一专长，在“网络防御”一章里，作者对安全攻防可谓“实话实说”。不乏烁见，发人深省。

当然，黑马并不是天才，Schneier 自己在后记中称，他的思想灵感是在成书前一年“显灵”的，在一年的时间里一边工作一边写作，要想将信息安全的真相搞得明明白白显然并非易事，书中不少章节也显露了作者理论和经验上的局限。比如在“对手”一章中，作者对计算机犯罪的概念仍显得有些书卷气，对攻击者的归类不太专长。在“证书和凭证”一章中，作者对 PKI/CA 的政策和证书管理讨论不够，也未提及时戳服务，第三方见证等可用于强化数字签名强度的措施。在“安全诀窍”一章中，作者对密码恢复的评论也不无偏颇。此外，“攻击树”一章虽然为风险评估提供了一个十分有益的理论模型，但是作者提出的信息安全风险的评估方式是否实用尚难断言。

尽管如此，本书与《应用密码学》一样自推出以来，畅销不衰。成为 2000 年信息安全领域的热门话题。机械工业出版社购得了本书的中文出版权，并诚邀我们翻译。我们为机械工业出版社翻译过《应用密码学》，原以为驾轻就熟，殊不知 Schneier 先生在本书中文风突变，采用的是灵活、风趣的非技术语言。这给我们的翻译工作提出了很大的挑战。必须承认，由于水平所限，要在很短的时限内完全转达该书的风格是相当困难的，所以对书中的误译和错译，请读者一定见谅。我们诚挚地推荐专业人士能读本书的原著。

此外，本书的全名为“秘密与谎言：网络化世界中的数字安全”我们觉得太长，也太文学化，根据我们对本书的理解，故且将书名译为《网络信息安全的真相》，不知是否妥当、贴切。

译者

2001 年 9 月

于北京昆明湖畔

前　言

我写这本书，部分原因是为了纠正一个错误。

7年前，我写了一本书：《Applied Cryptography》(《应用密码学》,中译本由机械工业出版社出版)。在该书中，我描述了一个数学的乌托邦：密码算法能将你最深的秘密保持数千年，安全协议能安全而可靠地执行最难以想象的电子交互，如不规则的赌博、不可检测的认证、匿名货币等。根据我的观点，密码学是超凡的技术均衡器，任何人只要有一台便宜的（而且越来越便宜）计算机，就可以达到与最强大的政府同样的安全性。在两年以后该书的第二版内，我进一步写道："仅靠法律保护我们自己还远远不够，我们还需要用数学保护我们自己。"

事实并非如此，密码学并不能做那么多的事情。

并不是说密码学从1994年开始变得软弱，也不是说我在那本书中描述的不再是真的，我想说的是密码学并非存在于真空之中。

密码学是数学的一个分支。像所有其他数学分支一样，它涉及的是数字、公式和逻辑。安全性，特别是在我们的生活中十分有用的安全性，它涉及的是人：人所知道的事情、人与人之间的关系、人和机器的关系。而数字的安全性涉及到的是计算机：复杂的、不稳定的、充满漏洞的计算机。

数学是完美的，而现实却是主观的。数学是精确的，而计算机却充满矛盾。数学是遵循逻辑的，而人却是不稳定的、反复无常的，甚至是难以理解的。

《Applied Cryptography》的错误是由于我完全没有讲到前后关系，我把密码学说成了灵丹妙药，我真是有些天真。

结果可想而知。广大读者将密码学视为一种神奇的安全性粉面，认为把它洒在软件上，就可以使软件安全。这样，他们就会依恋神奇的说法，例如"128位密钥"和"公开密钥基础设施"(PKI)。有位同事曾告诉我，世界上充满着读了《Applied Cryptography》的人设计的安全性很糟的系统。

自从写了那本书后，我就成为了密码学顾问，并不断设计和分析安全性系统。但让我深感震惊的是，安全性的弱点与数学毫无关系，它们存在于硬件、软件、网络以及人的身上。数学的完美与糟糕的编程、极差的操作系统和一个人的口令字选择不当没有关系。我学着从密码学以外的角度去思考，从整个系统中发现弱点。从这本书中，你将会看到我反复提出的一些观点："安全性是一条链，其可靠程度取决于链中最薄弱的环节"。"安全性是一个过程，而不是产品"。

现实世界的任何系统都是一串复杂的环节，安全措施必须渗透到系统的所有地方：它的组件和连接。在本书中，我要阐明的是现代系统有太多的组件和连接，其中一些甚至连系统的设计者、实现者和使用者都不知道。因此，不安全因素总是存在。没有一个系统是完美的，

没有一项技术是灵丹妙药。

对每一个与现实有关系的人来说，这一点很显然。在现实世界中，安全性涉及到过程。它涉及到预防性技术，也涉及到检测和反应过程，以及一个完整的追查和检控犯罪的侦察制度。安全性不是产品，它本身是一个过程。如果要使我们的数字系统安全，就必须完整构建这一过程。

几年以前，我听到一句箴言，我在这里将它修改为：如果你认为技术能解决安全性问题，那么你就不理解安全性问题，也不理解技术。

本书要论述的就是这些安全性问题、技术的局限性以及解决方案。

请从头到尾，按顺序阅读本书。

许多技术书籍可以来回跳着看，作为参考资料使用，不需要按顺序阅读，真的不需要。而本书则不是这样。本书有情节，像一个故事。像任何好故事一样，如果不按顺序讲，几乎没有什么意义。每一章都是前后相关的，如果你不走完全程，你就不能获得最终结果。

实际上，我要求你从头到尾阅读两次。本书想说明的是，为了理解系统的安全性，你应当观察整个系统——而不是任何一项特定的技术。安全性本身是相互连接的系统，在详细了解任何一件事之前，最好能粗略地了解所有的事。但是，要求读两遍可能是太过苛求，请原谅我提出了这个要求。

本书共分三部分：第一部分是“前景”，它给出了本书其余部分的背景：谁是攻击者，他们要做什么，我们怎样对待威胁。第二部分是“技术”，它基本上是一些叙述不同的安全性技术和它们的局限性的章节。第三部分是“策略”，在知道了概况中的要求和技术的局限性后该做什么。

我认为数字安全是当今最酷的事，本书表达了这种感觉。它十分艰难，但充满乐趣。请从阅读本书中享受这种乐趣吧。

目　录

第1章 引 言

在2000年的3月间，我记录了来自各种消息源的安全事件。以下是新闻摘要：

某人闯入了SalesGate. com的B2B（business-to-business）网站，窃取了约3000名客户的记录，其中包括信用卡号以及其他个人信息。此人还在互联网上张贴了其中一些人的资料。

数年来，个人信息一直被从网站（如Intuit）上泄露给广告商（如DoubleClick）。当访问者在Intuit网站上使用各种财务计算器时，网站程序中的一个小的设计差错就会把用户输入的信息传送给DoubleClick。这种情况是在用户不知情或者未经用户同意时发生的，而且（更加令人感到吃惊）Intuint对此也同样是不知情或者未经过它的同意。

被判犯罪的黑客Kevin Mitnick在立法机关面前服法。他告诉他们，社会工程是一个主要的安全薄弱环节：他经常只需假装成其他人进行询问，就会得到密码及其他的秘密。

Gallup（盖洛普）民意调查表明，三分之一的在线客户表示受到了最近发生的计算机安全事件的影响，他们有可能不愿意从网站购物。

从索尼公司（Sony）网站订购PlayStation 2客户的个人资料曾被意外地泄露给其他的客户（实际上这是所有网站都不能控制的问题。人们在结账时，却会看到另一位网络客户的信息内容）。

Amazon. com为第三方网站提供的转荐服务支付佣金。某人发现的一种破坏管理此操作程序的方法，能够让任何人将信息传送给各种人。Amazon是否将此视为问题还不得而知。

美国中央情报局的主管否认美国涉嫌经济间谍活动，不过并未继续否认名为ECHELON的大规模情报收集系统的存在。

22岁的Pierre-Guy Lavoie因闯入数台加拿大和美国政府的计算机，而在魁北克被定罪。他将在监狱服刑12个月。

日本国防机构在发现奥姆真理教的狂热分子已开发出相关软件之后，推迟布署一种新型的计算机防御系统。

一种名为Pretty Park的新型电子邮件蠕虫在互联网上广为蔓延。它只是对去年出现的同类病毒进行了微小的改动。它通过把自己传送给用户的Outlook Express程序的地址表中的所有地址，自动进行传播。

Novell和Microsoft继续就利用Windows 2000的现有活动目录的一个可疑的安全臭虫展开针尖对麦芒式的交锋。这是否成为一个真正的问题取决于你从你的目录中所期待的安全属性（我认为这是Windows中的一个设计缺陷，而不是一个臭虫）。

在西西里岛的两个人（Giuseppe Russo和他的妻子Sandra Elazar）因在互联网上偷盗了约1500个信用卡号，并用它们购买奢侈品及彩票而被捕。

名为“Coolio”的黑客（实际上是一个令人讨厌的青少年）否认在2000年2月里发起了

大规模的拒绝接入服务型的攻击。他承认在过去曾破坏性闯入过约 100 个网站，其中包括长于加密的 RSA 安全公司，以及属于美国国务院的一家网站。

攻击者针对 Microsoft 的以色列网站发起了一次拒绝接受服务型的攻击。

别名为“The Gatsby”的 Jonathan Bosanac 因破坏性闯入三家电话公司的网站，而被判刑 18 个月。

以下是 2000 年 3 月期间，关于某些软件的缺陷报告：

有报告称 Microsoft Internet Explorer 5．0（在 Windows 95、98、NT4．0 以及 2000 里都有）中的缺陷允许攻击者建立一个网页，并可执行访问者计算机中的任何程序。

通过修改 URL（统一资源定位符），攻击者可以完全避开保护 Axis StarPoint CD-ROM 服务器的远程管理屏的鉴别机制。

如果一名攻击者向 Netscape Enterprise Server 3．6 发送特定类型的长消息，缓冲区的溢出就会破坏一个特定的程序。攻击者也就能以远程方式在服务器上随心所欲地执行代码。

完全有可能发起互联网安全系统（ISS）公司的 RealSecure 网络入侵检测软件无法检测出来的攻击（一种为拒绝服务型的攻击，另一种为针对 CGI 脚本的攻击）。

攻击者通过把一个特定的 URL 发送给运行着 Alliaire 的 ColdFusion 产品的服务器，就可以接收到一个关于各种文件的物理路径的出错消息。

Omniback 是惠普公司的一个产品，用于定期执行系统备份。攻击者可以对此产品做手脚，造成拒绝服务型攻击。

Dosemu 是随 Corel Linux 1．0 配备的 DOS 仿真程序。在 Dosemu 的配置中也存在缺陷，它允许用户以根优先权执行命令。

攻击者只要修改特定的变量内容，就可以利用 DNSTools 1．0．8 中的缺陷执行任意代码。

SGI 有一个名为 InfoSearch 的信息包，它可以自动地把文本文件转换成 HTML Web 内容。CGI 脚本中的一个臭虫允许攻击者在服务器上以网络服务器的优先权级别执行命令。

在电子邮件客户机 The Bat！中也发现了数个缺陷，它们允许攻击者从用户的计算机中偷取文件。

Microsoft 的剪贴画功能可让用户从网络上下载剪贴画文件。在特定的环境下，一个变形的剪贴画文件可以让任何代码在用户的计算机上运行。

如果向 Bison Ware 的 FTP Server 3．5 发送一个长的登录名和密码（甚至是一个错误的密码），它就会崩溃。

入侵者可以使用特殊编码的 URL，令 Windows 95 和 98 计算机崩溃。

下面是 attrition．org 网站上列出的、于 2000 年 3 月期间被涂毁的 65 家知名网站的清单。在本文中，“被涂毁”意味着某人闯入了网站，并且修改了主页：

Tee Plus; Suede Records; Masan City Hall; The Gallup Organization; Wired Connection; Vanier College; Name Our Child; Mashal Books; Laboratorio de Matematica Aplicada da Universidade Federal do Rio de Janeiro; Elite Calendar; Centro de Processamento de Dados do Rio de Janeiro; Parliament of India; United Network for Organ Sharing; UK Jobs; Tennessee State University; St．Louis Metropolitan Sewer District; College of the Siskiyous; Russian Scientific Center

for Legal Information, Ministry of Justice; RomTec Plc; Race Lesotho; Monmouth College; University of St. Thomas Library; Int Idea Sweden; Goddard College; Association of EDI Users; Bitstop, Inc; Custom Systems; Classic Amiga; 98 Skate; CUNaked; Korea National University of Education; PlayStation 2; Association for Windows NT System Professionals; K. Net Telecomunicações Ltda.; CyberCT Malaysia; Birmingham Windows NT User Group; Bloem S. A.; Aware, Inc.; Ahmedabad Telephone Online Directory, Ahmedabad Telecom District; Fly Pakistan; Quality Business Solutions; Out; Internet Exposure; Belgium Province de Hainaut; Glen Cove School District; Germantown Academy; Federatie van Wervings en Selectiebureaus; Engineering Export Promotion Council, Ministry of Commerce, India; AntiOnline's AntiCode; Pigman; Lasani; What Online; Weston High School; Vasco Boutique; True Systems; Siemens Italy; Progress Korea; Phase Devices Ltd.; National Treasury Employees Union; National Postal Mail Handlers Union; Metricks; Massachusetts Higher Education Network; The London Institute; Fort Campbell School System; and MaxiData Tecnologia e Informatica Ltda.

最后，我的一位朋友的家用计算机，通过有线调制解调器上网，也受到了攻击：

- 有 26 次扫描，寻找可利用的缺陷。
- 有 4 次特别坚定的闯入这台计算机的企图，其中包括基本缺陷扫描以及成堆的、其他狡猾的黑客伎俩。

实际上，清单上的攻击只是发生在 2000 年 3 月的 1 号到 7 号这几天里。此后我就厌倦了保留此类记录。

浏览了这个清单之后，令我震惊的是问题、缺陷以及攻击的范围是如此之广。这些缺陷有的位于据称是安全的软件产品中，有些缺陷则位于经过了安全设计的电子商务系统中。某些缺陷是在新产品中，还有其他的缺陷则位于销售多年的产品之中。有时供应商甚至不承认这些问题存在。

2000 年 3 月的头 7 天并非特例。其他数周也有类似的记录，有些记录则更糟。实际上，资料显示情况正变得更加糟糕：安全缺陷、侵犯以及灾难性事件的数量正随着时间的推移而增加。我们学会有关安全的东西越多——如何设计加密算法、如何建立安全的操作系统等，我们建立的系统越不安全。为什么会这样，我们应怎么办，这正是本书的主题。

1.1 系统

“系统”的概念对于科学而言还相对较新。东方的哲学家很早以前就将世界视为一个由各种要素组成的单个系统，不过西方的哲学家则把世界分割成以不同方式相互作用的独立事物。

机器是最近才成为系统的。滑轮是一台机器；电梯是由许多不同机器构成的一个复杂的系统。各种系统是相互作用的：电梯与大楼内的电气系统、消防系统，甚至还可能有环境控制系统相互作用。计算机相互作用形成网络，而网络也相互作用形成更大的网络，个中道理不难理解。

海军上将 Grace Hopper 说过："二战前的世界还很简单，二战后我们才有了系统"。这一评论具有深刻见解。

一旦开始形成系统的概念，人们就可能在更加复杂的程度上设计并建立系统。这是大楼与摩天大厦之间，加农炮与爱国者导弹之间，降落跑道与飞机场之间的根本差别。任何人都可以设立一个交通信号灯，但是要设计一个全市的交通控制系统则远非常人所能。

互联网可能是至今发展出的、最为复杂的系统。它将数百万台计算机连接到一个复杂得令人难以想像的物理网络上。每台计算机中有数百个在其上运行的软件程序；其中的一些程序与此计算机上的其他程序相互作用，另一些程序则穿过网络与其他计算机上的其他程序相互作用。该系统从数百万人那里接收用户输入，有时则同时接收所有的输入。

正像人们常说的："先生，就像看狗站立，让人惊讶的不是站得好不好，而是它是否站起来"。

本书将介绍系统的很多有趣属性。

首先是复杂性。机器相对简单：一个锤子，一个门折页，一把切牛排的小刀。系统则要复杂得多，它们有零件、反馈环路、故障的平均时间、基础结构等。数字系统则是错综复杂的；即便是一个简单的计算机程序也会有数十万行的计算机代码，执行各种不同的操作。一个复杂的计算机程序有数千个构成要素，每个构成要素都得自己运行，并且与其他所有的构成要素相互作用。这就是开发面向对象的编程方式的原因：处理数字系统的复杂性。

其次，系统之间彼此相互作用，形成更大的系统。这种情况可以有目的地实现，比如程序员采用不同对象把大系统拆分成小一些的系统，工程师把大的机械系统拆分成小型的子系统，等等。这种情况还可以自然发生，如汽车的发明，导致现代道路与高速公路系统的发展，而且这种发展又依次与我们日常生活中的其他系统相互作用，从而产生了郊区。航空交通控制系统与飞机上的导航系统和天气预报系统相互作用。人体与人体之间以及人体与地球上的其他系统相互作用。互联网将自身与我们社会中的每个重要系统都联系在一起。

第三，系统有新兴的属性。换言之，它们做了用户或设计者未能预期到的事情。例如，电话系统改变了人们的相互影响方式（Alexander Graham Bell 当时并没有想到电话是一个个人通信设施；他认为你能够用它提前发出有电报的通知）。汽车改变了人们会面、约会，以及恋爱的方式。大楼中的环境控制系统对人们的健康有影响，而这又会影响到保健系统。字处理系统改变了人们书写的方式。互联网中充满了新兴的属性；想想 eBay、虚拟性爱、合作授权等。

第四，系统有臭虫或缺陷。臭虫是一种特殊的失误。它是系统的一个新兴属性，不过是不值得人向往的那种，它不同于故障。当某东西出故障时，它不能再正常运行。当某东西有臭虫时，它就以一种特殊的方式采取不端行为，可能无法重复，而且可能无法解释。臭虫是系统独有的属性。机器可以损坏、出故障或不运行，但是只有系统才会有臭虫。

1.2　系统与安全

上述属性都对系统的安全有深远的影响。目前要给"安全"一个精确的定义还相当困难，原因是保证一个像互联网这样的复杂系统的安全极其困难，从根本上讲，这是因为它是一个复杂的系统。系统是很难实现安全的，而实现复杂系统的安全则更加困难。

对于计算机化的系统而言，通常的复制机制忽视了系统，而专注于单个计算机……技术。这就是我们在安全技术方面，如加密术、防火墙、公开密钥基础结构以及防篡改等等方面，还有大量工作要做的原因。这些技术更加易于理解、易于探讨，并且更加易于实现安全。这些技术都具有这种自负，即它们能够神秘地利用＜reverence type = “hushed” ＞ Secutity ＜/reverence＞属性深深影响系统。

事实并不尽然，结果可以从我 2000 年 3 月头 7 天的安全记录中看到。大多数安全事件可以归于先前列出的 4 个系统属性中的一个或多个。

复杂性。Windows 2000 的现有活动目录中的安全问题可以直接归于任何基于计算机的目录系统的复杂性。这就是我认为它是一个设计缺陷的原因；Microsoft 制定了一个能够促进可用性的设计方案，却损害了安全。

交互性。Intuit 网站上的软件与 DoubleClick 用来向网络用户显示广告的软件之间的相互影响导致信息从一个人那里泄露到另一个人那里。

创新性。据新闻报道说，Sony 的程序员并没有想到信用卡信息会从一个用户泄露到另一个用户那里，它却恰恰发生了。

隐含的臭虫。Netscape Enterprise Server 3．6 中的缺陷是由一个程序臭虫导致的。攻击者能够利用这个臭虫引发安全问题。

本书中的许多内容（尤其在第 3 部分中）专门详细解释了安全应该被视为较大系统中的一个系统的原因，不过，我愿意你从开始起就把这两件事情铭记在心。

首先是安全理论与安全实践之间的关系。在安全理论方面有大量重大的理论支持，却输于实践的检验。

Yogi Berra 曾经说过：“从理论上说理论与实践之间没有差异，但在实践中，两者却是有差异的。”

理论在理想条件和实验室环境中能够起到最佳的作用。出自我校物理系中的一则流行笑话是“假设一只球形的、统一密度的母牛”。我们只能够在理想化的系统中做计算。现实世界要比理论世界复杂得多。数字系统的安全也是同样的：我们可以设计理想化的、证明是可靠的操作系统，但是我们却不能真正建立这些系统，让它们在现实世界中安全地运行。现实世界涉及到设计中的折衷、没有预见的变量以及不完美的实施等。

现实的系统并不会改变自身以适合理论上的推导，只有老式学校的学究们才会唯理至上。球形母牛必须与现实的 Holstein 具有相同的新兴特征才行，但事实并非如此。因而科学家就是科学家，而不是工程师。

第二个要铭记在心的事情，是预防、检测与做出反应之间的关系。好的安全性能包括以下所有内容：一个保护财富的保险库，检测到试图打开保险库的盗贼时就会发出警报，警察会及时对警报做出反应，并逮捕盗贼。数字安全系统趋向于完全依赖预防：加密术、防火墙以及其他等等，通常没有检测，而且几乎没有任何响应或审查。一个只预防的策略只是在预防机制完美无缺的情况下才起作用；否则有人将会找出如何避开它们的方法。本章中列出的大多数攻击及缺陷都是避开预防机制的结果。面对这种已知的现实情况，检测与响应就变得至关重要。

第一部分 前 景

计算机安全通常以抽象的广告形式出现："该系统是安全的"。产品供应商可能会说："本产品能够保护你的网络安全"，或者说："我们能够保护电子商务的安全"。上述断言显然十分天真和过于简单。这些产品供应商们着眼的是产品的安全，而不是系统的安全。对此需要最先提出的问题是："安全来自于谁?"以及"安全是针对什么的?"。

这些都是真正的问题。不妨试想一位销售安全操作系统的厂商，他能安全阻止手榴弹落到CPU上吗？能够阻止某人直接将视频摄像头放到键盘及显示屏后面吗？能够阻止某人渗透到公司中吗？恐怕不能；这并不是因为操作系统有缺陷，而是因为有人有意、无意地制定了各种设计方案，而这些方案正与该操作系统要阻止的各类攻击以及忽视的各类攻击有关。

如果未经深思就制订了上述方案，问题就会随之而来，而且这些问题并不总像前面示例那样具体明了。一台安全的电话是要阻止一个临时的听众、一个资金充足的窃听者或者一个国家的情报机构？一家安全的银行系统是要阻止客户行骗、商家行骗、出纳员行骗还是银行经理的行骗呢？一旦使用了另外的产品，是否就能提高或降低各种安全所需的安全性呢？对许多人而言，某种特殊的安全技术到底能做什么不能做什么，实在是太深奥了。

安全从来就不是一种非白即黑的概念，其背景关系远比技术更重要。比如一个安全的操作系统无法阻止手榴弹的原因并不意味着它就无用；相反它意味着我们不能没有墙、门锁及窗户栏杆儿。不同的安全技术在一个综合的安全方案中占有不同的重要地位。一种系统可能能够利用特定的技术装置，阻止普通的罪犯，或是一定类型的产业间谍，或是一个国家级情报机构的侵犯。只要不出现特定的数学进步，或者在某一个特定的时期内，或者针对特定类型的攻击而言，一种系统可能会是安全的。与任何的形容性词汇一样，脱离了背景的"安全"是毫无意义的。

在这一部分的各章中，我打算介绍这种背景的基本内容。我会谈到针对数字系统的威胁、攻击的类型以及攻击者的类型等。此后我还会谈到安全的迫切之需。我在讨论各种技术之前做这些介绍，是因为你在没有前景意识的情况下，无法理智地检测各种安全技术。就像未置身于中世纪当中，就无法理解城堡在地区防御中所起的作用一样，你在互联网的背景之外，就无法理解防火墙或一个加密的互联网连接在网络世界中所起的作用。谁是攻击者？他们想要什么？他们的配置中有何种工具？不了解这些基本的内容，你就无法以合理的方式探讨任何保护事物的安全方式。

第2章 数字威胁

世界到处充满了危险。如果你在一条昏暗的小道上漫步，劫匪可能会扑向你；高超的骗