《信息安全原理与实践（第2版）》

图书基本信息

书名：《信息安全原理与实践（第2版）》

13位ISBN编号：9787302317852

10位ISBN编号：7302317852

出版时间：2013-5

出版社：清华大学出版社

作者：【美】斯坦普(Stamp, M.)

页数：463

译者：张戈

《信息安全原理与实践（第2版）》

内容概要

面向21世纪的信息安全指南
信息安全是一个快速发展的领域。着眼于最富时代感的安全议题，涵盖涉及宽泛的一系列新鲜信息，这本经过充分更新和全面修订的《信息安全原理与实践(第2版)》为读者提供了解决任何信息安全难题所必备的知识和技能。
主要内容
通过聚焦于现实世界中的生动实例，并采用一种面向实践的信息安全讲述方法，这本书围绕如下4个重要主题进行组织并展开：
密码学技术：包括经典密码系统、对称密钥加密技术、公开密钥加密技术、哈希函数、随机数技术、信息隐藏技术以及密码分析技术等。
访问控制：包括身份认证和授权、基于口令的安全、访问控制列表和访问能力列表、多级安全性和分隔项技术、隐藏通道和接口控制、诸如BLP和Biba之类的安全模型、防火墙以及入侵检测系统等。
协议：包括简单身份认证协议、会话密钥、完全正向保密、时间戳技术、SSH协议、SSL协议、IPSec协议、Kerberos协议、WEP协议以及GSM协议等。
软件安全：包括软件缺陷和恶意软件、缓冲区溢出、病毒和蠕虫、恶意软件检测、软件逆向工程、数字版权管理、安全软件开发以及操作系统安全等。
在本书第2版中，特别引入了一些比较新的内容，其中涉及的安全主题包括SSH协议和WEP协议、实际的RSA计时攻击技术、僵尸网络以及安全证书等。同时还增加了一些新的背景知识，包括Enigma密码机以及一部分关于经典“橘皮书”之安全观的内容。此外，本书还有一大特色，就是大幅度地扩展和更新课后思考题，并增补了许多新的图解、表格和图形，用以阐明和澄清一些复杂的主题和问题。最后，对于课程开发来说，还有一组综合性的课堂测试用的PowerPoint幻灯片文件以及问题解答手册可供利用。

《信息安全原理与实践（第2版）》

作者简介

作 者 简 介
我在信息安全领域已有将近20年的经验了，其中包括在行业中和政府里从事的一些宽泛的工作内容。我的职业经历包括在美国国家安全局(National Security Agency，NSA)的7年多，以及随后在一家硅谷创业公司的两年时间。虽然关于我在NSA的工作，我不能说太多，但是我可以告诉你——我的职业头衔曾经是密码技术数学家。在这个行业当中，我参与设计并开发了一款数字版权管理安全产品。这段现实世界中的工作经历，就像三明治一样被夹在学术性的职业生涯之间。身处学术界时，我的研究兴趣则包含了各式各样广泛的安全主题。
当我于2002年重返学术界时，于我而言，似乎没有一本可用的安全教科书能够与现实世界紧密相连。我觉得我可以撰写一本信息安全方面的书籍，以填补这个空缺，同时还可以在书中包含一些对于处于职业生涯的IT专业人士有所裨益的信息。基于我已经接收到的反馈情况，第1版显然已经获得了成功。我相信，从既是一本教科书，又可作为专业人员的工作参考这个双重角色来看，第2版将会被证明更具价值，但是因此我也会产生一些偏见。可以说，我以前的很多学生如今都从业于一些领先的硅谷科技公司。他们告诉我，在我的课程中学到的知识曾令他们受益匪浅。于是，我当然就会很希望，当我之前在业界工作时也能有一本类似这样的书籍作为参考，那样我的同事们和我就也能够受惠于此了。
除了信息安全之外，我当然还有自己的生活。我的家人包括我的妻子Melody，两个很棒的儿子Austin(他的名字首字母是AES)和Miles(感谢Melody，他的名字首字母不至于成为DES)。我们热爱户外运动，定期会在附近做一些短途的旅行，从事一些诸如骑自行车、登山远足、露营以及钓鱼之类的活动。此外，我还花了太多的时间，用在我位于Santa Cruz山间的一座待修缮的房子上。

《信息安全原理与实践（第2版）》

书籍目录

《信息安全原理与实践（第2版）》

精彩书评

1、有些信息安全的教科书会堆砌大块干燥乏味且一无是处的理论说辞。任何一本这样的著作，读来都会像研读一本微积分教材那般充满刺激和挑战。另外的一些读本所提供的内容，则看起来就像是一种对于信息的随机性收集，而其中的信息却是显然毫不相干的事实罗列。这就会给人们留下一种印象，安全实际上根本不是一个有机结合的主题。而这本书则是着眼于对实践问题的研究，同时尽量覆盖了足够多的基本原理，以备可以在这个领域中展开更深入的研究。并且也力争尽可能地最小化所需要的背景知识。特别是，对于数学形式的表达，已经控制到了最低限度。

《信息安全原理与实践（第2版）》

版权说明