# <<系统安全工艺>>

## 图书基本信息

书名：<<系统安全工艺>>

13位ISBN编号：9787302194729

10位ISBN编号：7302194726

出版时间：2009-4

出版时间：SeanSmith、John Marchesini、黄清元、 李化 清华大学出版社 (2009-04出版)

作者：SeanSmith，John Marchesini 著

页数：380

## 前言

“我认为这本《系统安全工艺》是当今市面上最棒的软件安全书籍之一。
其内容广而深、覆盖的内容有密码学、网络构建、操作系统、Web、人机交互、以及如何通过改进硬件来提高软件系统安全性。
简而言之，《系统安全工艺》适合所有系统安全从业者，并且也可以选作大学计算机科学课程的教材。
”——Edward Bonver，CISSP（信息系统安全认证专业人员）、Symantec公司产品安全的资深QA工程师“这将会是一次有趣的、令人兴奋的阅读：该书囊括了各种有关计算机安全应用和误用的实例，是一本独特而新颖的书籍。
我期望《系统安全工艺》能够激发广大学生朋友投身到安全技术领域中来；同时，该书还能够满足安全专家们的需要。
”——L.Felipe Perrone，Bucknell大学计算机科学系教授过去，仅有专家对计算机安全感兴趣，但是，现在它已经成为社会中每个人都需要关注的内容。
生活中经常需要计算，一旦计算机遭到破坏将会引发非常严重的后果。
但试图掌控计算中的全部细节问题几乎是不可能的，参与计算的多个方面都存在复杂性问题，如独立构件和计算硬件、操作系统、应用程序、网络协议，以及使用这些系统的人为因素等。
安全是每个人都应关注的问题，一个非常直接的问题是如何让每个参与者都明白安全方面的知识和安全的重要性。
从软件工程师、经理、律师，以及任何其他人的职业生涯可以看出，研究者和从业者不仅需要关注安全涉及的广度，还需要关注其深度，如安全的发展趋势和准则等。
现在，安全研究文献过多关注于系统管理、密码学体制、桔皮书或者NSA标准，计算机科学研究人员和计算机安全从业人员能够轻易地发现详细描述某些特定工具的书籍，这些工具可以用来对系统安全性进行评估，但是，这些书籍并没有向读者阐述更为本质的问题：人们为什么要开发这些工具？
如何和何时使用恰当的工具来解决特定的问题。
此外，现有文献也无法辅助人们开发出安全的系统，很多工具能够有效地辅助系统审计员进行审计，但对于安全系统开发人员则没有帮助。

# <<系统安全工艺>>

## 内容概要

《系统安全工艺》首先快速回顾了计算机安全方面的历史，随后窥视了安全的前景，展示了安全的新挑战和如何应对这些挑战，并提供了一套体系以帮助理解当前的系统安全及其薄弱点。
接下来，《系统安全工艺》系统地介绍了构建系统安全的基本构建块，还将这些构建块运用到现在的应用中，并思考了当前涌现的一些重要技术，如基于硬件的安全技术等。
不论是系统安全从业者、开发人员、责任者还是管理员，都能够通过《系统安全工艺》更深层地理解安全形势以应对新的安全问题挑战。

## 作者简介

作者：(美国)SeanSmith (美国)John Marchesini 译者：黄清元 李化SeanSmith博士是Dartmouth大学的教授,负责教授计算机科学和研究真实世界可信系统的开发，他所致力的项目(研究GoodSamaritans对wikipedia的影响)被NetworkWodd杂志评选为25大最酷，最前沿的IT研究项目之一，他投身子信息安全方向的研究已15年，拥有多项专利成果，著有TrustedComputing.Platforms：DesignandApplications一书。
JohnMarchesini博士，拥有休斯顿大学的硕士学位和达特茅斯学院的计算机科学博士学位，他曾经是Symantec公司的资深安全工程师，还是产品安全组的一员，现在是EminentWareLLC的首席安全架构师。

# <<系统安全工艺>>

## 书籍目录

第1部分 历史背景第1章 安全概述1.1 安全的传统定义1.2 访问控制矩阵1.3 其他观点1.4 安全状态和访问控制矩阵1.5 其他安全难题1.6 本章小结1.7 思考和实践第2章 旧约2.1 基本框架2.2 安全模型2.3 桔皮书2.4 信息安全.作业安全和工作安全2.5 本章小结2.6 思考和实践第3章 旧准则,新环境3.1 桔皮书是否解决了错误问题3.2 是否因缺乏政府支持而虎头蛇尾3.3 旧准则是否太不实用3.4 Saltzer牙口SChrOeder3.5 旧准则在现代计算环境中的适用性3.6 本章小结3.7 思考和实践第Ⅱ部分　安全与现代计算场景第4章 操作系统安全4.1 操作系统的背景4.2 操作系统安全的基本概念和原理4.3 真实操作系统：几乎实现了所有功能4.4 针对操作系统的攻击4.5 选择何种操作系统4.6 本章小结4.7 思考和实践第5章 网络安全5.1 基本框架5.2 协议5.3 网络攻防5.4 新技术.新问题5.5 本章小结5.6 思考和实践第6章 安全实现6.1 缓冲区溢出6.2 参数验证和其他问题6.3 TOCTOU6.4 恶意软件6.5 编程语言安全6.6 开发周期内的安全6.7 本章小结6.8 思考与实践第Ⅲ部分 安全系统的构成模块第7章 密码学7.1 框架和术语7.2 随机化7.3 对称密码学7.4 对称密码学的应用7.5 公钥密码学7.6 hash函数7.7 公钥的实现问题7.8 过去和未来7.9 本章小结7.10 思考与实践第8章 密码破解8.1 非暴力破解对称密钥8.2 暴力破解对称密钥8.3 非因式分解方法破解公钥8.4 密码机制实现破解8.5 模数分解的可能性8.6 本章小结8.7 思考与实践第9章 身份认证9.1 基本框架9.2 人的身份认证9.3 人为因素9.4 从机器的角度看身份认证9.5 高级方法9.6 案例研究9.7 其他问题9.8 本章小结9.9 思考与实践第10章 公钥基础设施.10.1 基本定义10.2 基本结构10.3 复杂性10.4 多证书中心lO.5 证书回收10.6 X.5 09方案10.7 反对观点10.8 当前存在的问题10.9 本章小结10.10 思考与实践第11章 标准、实施和测试11.1 标准11.2 策略实施11.3 测试11.4 本章小结11.5 思考和实践第Ⅳ部分 应用第12章 Web及其安全12.1 基本结构12.2 安全技术12.3 隐私问题12.4 Web服务12.5 本章小结12.6 思考与实践第13章 办公工具及其安全13.1 Word13.2 Lotus1-2-313.3 PDF13.4 剪切-粘贴13.5 PKI和办公工具13.6 概念模型13.7 本章小结13.8 思考与实践第14章 货币、时间、属性14.1 货币14.2 1时间14.3 属性14.4 本章小结14.5 思考与实践第Ⅴ部分新型工具第15章 形式化方法和安全15.1 规范15.2 逻辑15.3 实现15.4 案例研究15.5 了解你的银行账号15.6 自动形式化方法的不足15.7 本章小结15.8 思考与实践第16章 基于硬件的安全16.1 数据残留16.2 攻击和防御16.3 工具16.4 其他体系结构16.5 发展趋势16.6 本章小结16.7 思考与实践第17章 搜索有害位17.1 AI工具17.2 应用分类17.3 案例研究17.4 实坝17.5 本章小结17.6 思考与实践第18章 人为因素18.1 最后一程18.2 设计准则18.3 其他因素18.4 信任18.5 本章小结18.6 思考与实践附录A 相关理论A.1 关系、序、格A.2 函数A.3 可计算性理论A.4 框架A.5 量广物理和量子计算参考文献

## 章节摘录

插图：从定义上来看，广域网是范围较广的网络。
如果按照每英尺的开销来看，广域网虽然速度较慢，但也比较便宜。
现实的广域网所使用的介质要超出人们的想象：电话线、卫星等。
广域网络也引发了一些范围较大时需要关注的问题，如拓扑和分割。
现实世界的网络拓扑非常有趣。
例如，美国的电信网络最近出现了异常，就是由网络拓扑的概念模型和物理真实模型不匹配引发的；有人设法破坏了关键网络线路和其备用线路，通过复杂的业务关系，最终也会引发网络拓扑概念模型与物理真实模型的不匹配。
另外一个例子，人们在绘制广域网络拓扑时发现，企业之间的链接有聚合的趋势，但是为什么出现聚合则原因不明。
5.1.2查找联网机器一旦有大量的机器参与网络互联，下一步就是设法找到那些机器。
首先，需要命名这些机器，即主机名（hostname）。
主机名是人类可理解的机器名，如WWW.CS.dartmouth.edu。
这些名称遵循特定的层次结构：.edu域、在该域的.dartmouth组织以及.cs子组。
简单说来，主机名是唯一的，每台机器对应一个主机名，反之亦然。
但实际中可能并非如此，例如，一个服务器名可能对应很多台主机，这主要是出于负载均衡的考虑，一台机器也可能有两个不同的名称。

# <<系统安全工艺>>

## 编辑推荐

《系统安全工艺》是深受读者喜爱的。
权威专家旁征博引，深入剖析安全体系的竭诚之作最新的系统安全及其薄弱点的详细说明；为全面认识安全体系，拥有解决问题的敏锐思维铺路搭桥内容涉猎广泛，叙述客观、生动，见解独到

## 版权说明