

<<可信计算平台>>

图书基本信息

书名：<<可信计算平台>>

13位ISBN编号：9787302131748

10位ISBN编号：7302131740

出版时间：2006-1

出版时间：清华大学

作者：[美] 史密斯 (Smith, S.

页数：204

字数：300000

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<可信计算平台>>

### 内容概要

本书是国际上可信计算领域出版的第一本专著，它从理论到实践，给出了该领域的技术发展脉络、关键设计技术和应用。

本书从可信计算平台需要解决的问题和相关需求出发，以作者亲自领导的一个可信计算平台实例（IBM 4758安全协处理器）的研发为主线，对可信计算平台的体系结构、设计和验证等关键技术进行了系统阐述，并且介绍了作者基于流行的TCG / TCPATPM芯片进行的前沿性实验工作和当前可信计算技术发展的一新方向。

本书并不局限于单一平台和相关规范的介绍，而是着眼于整个技术体系，力图从理论到实践给读者以全面的知识。

本书可以作为计算机、通信、信息安全、密码学等专业的研究生和本科生的教材，也可供从事相关专业的教学、科研和工程技术人员参考。

本书对从事可信计算平台设计、开发以及从事总体设计的人员来说也是一本难得的好书。

## 作者简介

Sean W. Smith目前在Dartmouth大学的计算机科学系任教，任Dartmouth安全技术研究所计算机安全与信任研究中心主任，以及Dartmouth PKI实验室的首席研究员。他当前的研究和教学的重点是构造现实世界中的可信系统。

## &lt;&lt;可信计算平台&gt;&gt;

## 书籍目录

第1章 引论 1.1 信任与计算 1.2 可信计算平台的实例 1.3 设计与应用 1.4 本书结构第2章 动机说明  
2.1 属性 2.2 基本用途 2.3 基本用途实例 2.4 放置和利益 2.5 TCP的放置实例 2.6 观点辩论 2.7  
进一步的阅读材料第3章 攻击 3.1 物理攻击 3.2 软件攻击 3.3 旁通道分析 3.4 未记录的功能 3.5  
擦除数据 3.6 系统环境 3.7 防御策略 3.8 进一步的阅读材料第4章 研究基础 4.1 应用和集成 4.2  
体系结构 4.3 启动 4.4 美国国防部及相关部门 4.5 进一步的阅读材料第5章 设计中的挑战 5.1 背景  
5.2 障碍 5.3 需求 5.4 技术选择 5.5 进一步的阅读材料第6章 平台体系结构 6.1 概述 6.2 清除秘  
密信息 6.3 秘密信息的起源 6.4 软件威胁 6.5 代码的完整性 6.6 代码的加载 6.7 总结 6.8 后续内  
容 6.9 进一步的阅读材料第7章 对外认证 7.1 问题 7.2 理论 7.3 设计和实现 7.4 进一步的阅读材  
料第8章 验证 8.1 验证过程 8.2 验证策略 8.3 安全属性的形式化描述 8.4 形式化验证 8.5 其他验  
证工作 8.6 反思 8.7 进一步的阅读材料第9章 应用案例研究 9.1 基本构造模块 9.2 增强型Web服务  
器 9.3 权限管理 9.4 私有信息保护 9.5 其他项目 9.6 经验 9.7 进一步的阅读材料第10章  
TCPA/TCG 10.1 基本结构 10.2 对外认证 10.3 物理攻击 10.4 应用 10.5 实验 10.6 TPM 1.2 的变  
化 10.7 进一步的阅读材料第11章 与TCPA/TCG有关的实验 11.1 预期的属性 11.2 生命周期不匹配  
11.3 体系结构 11.4 实现经历 11.5 应用：强化的Apache 11.6 应用：OpenCA 11.7 应用：隔离证  
明 11.8 进一步的阅读材料第12章 新的研究方向 12.1 特权体系结构 12.2 硬件研究 12.3 软件研究  
12.5 未来的工业平台 12.6 安全协处理回顾 12.7 进一步的阅读材料术语表参考文献关于作者

#### 版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>