

<<可信计算理论与实践>>

图书基本信息

书名：<<可信计算理论与实践>>

13位ISBN编号：9787302208754

10位ISBN编号：7302208751

出版时间：2009-10

出版时间：清华大学出版社

作者：冯登国 编

页数：177

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>

前言

随着计算机应用尤其是网络应用的普及，计算机病毒、恶意代码和黑客攻击事件层出不穷，通用计算机终端的安全问题越来越突出。

因此人们逐渐意识到必须从终端计算机的源头出发，综合采用安全芯片、硬件结构和操作系统等多种安全措施构建可信赖的计算环境，这就是可信计算的基本思想。

与传统的安全问题解决方法不同，可信计算从计算机体系结构着手，针对信息系统的安全需求和各种攻击手段，提出一种全新的体系结构级别的系统安全解决方案。

作为平台信任根的可信计算安全芯片提供了机密性、完整性、封装存储等一系列重要安全属性，这已经引起了产业界和学术界的极大兴趣，他们以极大的热情投身于可信计算核心技术和产品的研制，目前可信计算关键技术已经形成相当的积累。

国际上，1999年由HP、IBM、Intel、Microsoft等IT巨头成立了TCPA（Trusted Computing Platform Alliance），开始在全球范围内倡导可信计算理念，推广可信计算技术和标准。

2003年，TCPA改组为TCG（Trusted Computing Group），发布了TPM 1.2技术规范，同时从PC平台扩展到服务器、PDA、移动电话等各类平台，将可信计算技术渗透到可信计算平台的各个层面。

我国在可信计算领域起步不晚，发展也比较迅速。

在有关政府部门的认可和支持下，由众多厂商和科研机构共同成立了中国可信计算工作组（简称TCMU），大力发展自主创新的可信计算技术和标准。

目前我国已经成功研制了TCM（Trust Cryptographic Module）安全芯片、TSM（TCM Service Module）软件、安全PC等，全面地掌控了可信计算核心关键技术，并于2007年12月正式颁布了《可信计算密码支撑平台功能与接口规范》，标志着我国具有自主知识产权的可信计算技术、产品和标准进入一个新的发展阶段。

<<可信计算理论与实践>>

内容概要

《可信计算理论与实践：TCTP'2009（第一届中国可信理论与实践学术会议论文集）》为第一届中国可信计算理论与实践学术会议论文集，收录论文19篇，内容涉及可信计算的方方面面。主要内容包括可信计算密码理论和信任理论、可信计算体系结构、可信计算平台和可信系统、可信计算软件、可信网络及可信计算实践与应用技术等。

《可信计算理论与实践：TCTP'2009（第一届中国可信理论与实践学术会议论文集）》可供从事信息安全、密码学、计算机、软件、微电子、通信等专业的科技工作者和高等院校相关专业的师生参考。

<<可信计算理论与实践>>

书籍目录

A Remote Anonymous Attestation Scheme from ECCUCFS : Building a Usage Controlled File System with a Trusted Platform Module
A Direct Anonymous Attestation Scheme for Trusted Computing Platform Embedded with TCMTPM
中密钥迁移方案的安全性分析与改进
基于可信虚拟平台的配置更新方法
基于隐藏证书的远程证明方法
可信PDA计算平台系统结构与安全机制
可信计算平台在电力信息系统中的应用研究
可信计算平台中TOCTOU攻击的响应方法
可信网络连接研究
一种基于logistic混沌变换与奇异值分解的数字图像水印算法
一种基于标识认证的信任链建立方法
一种基于代理的直接匿名认证
一种基于可信度的可信网络接入体系结构
一种基于可信计算的分布式使用控制系统
一种基于无干扰模型的信任链传递分析方法
一种基于移动可信计算的软件下载框架
一种提高P2P网络可信性的信誉机制
移动终端基于TCM (Trusted Cryptography Module) 的内容保护管理

章节摘录

TPM中密钥迁移方案的安全性分析与改进 摘要：对TCG规范中密钥迁移方案的安全性进行了分析，结果表明，密钥迁移方案的安全性取决于密钥迁移过程中授权数据的安全性，而管理大量的、安全强度较高的授权数据并非易事。

针对这一问题，利用动态口令认证技术，在密钥迁移过程中引入动态迁移授权数据，将动态迁移授权数据与静态迁移授权数据相结合，提出了一种新的基于动态迁移授权数据的密钥迁移方案。

该方案不但增强了密钥迁移操作的安全性，而且降低了授权数据管理的复杂性，为用户提供了一种安全性高且易于管理的密钥迁移操作。

关键词：可信计算；密钥迁移；授权数据；动态口令 中图分类号：TP309文献标识码：A

1. 引言 密码技术是实现可信计算技术关键机制的基础，是可信计算技术的核心。

TCG规范规定了7种类型的密钥（大多为2048位的RSA密钥），包括背书密钥EK、身份证明密钥AIK、存储密钥、签名密钥、绑定密钥、继承密钥和鉴别密钥。

每种密钥都有一套约束来限制其使用，如每个平台只能拥有唯一EK，且只能用来在建立平台所有者时解密用户的授权数据，还有解密与生成AIK相关的数据，不能用于任何签名或加密。

<<可信计算理论与实践>>

编辑推荐

中国密码学会

<<可信计算理论与实践>>

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>